Lecture 2

Claim: If n is a positive integer, then $n^2 + 1$ is not a perfect square.

Proof: Let n be a positive integer. Then $n^2 < n^2 + 1 < n^2 + 2n + 1 = (n + 1)^2$. Since there are no integer squares between n^2 and $(n + 1)^2$, we are done. ■

Question: What if we change $n^2 + 1$ to $n^2 + 13$?

Note: When demonstrating this statement, we would need a proof. When showing the statement is false, we need a counterexample.

Solution: This is false. Consider what happens when $n = 6$. Then $n^2 + 13 = 6^2 + 13 = 49 = (7)^2$.

Question: What if we change $n^2 + 1$ to $1141n^2 + 1$?

Solution: This is true for all $n < 10^{24}$. Despite being true for a large number of values, this does not constitute a proof. It turns out in this case this is also false. Consider $n = 306933853227656571973972 08$. You can check this in Sage/Python that this does indeed give a counter example (that is, $1141n^2 + 1$ is a perfect square). Interested readers should check out Pell's Equations.

Instructor's Comments: This is the 12 minute mark

Definition: A *statement* is a sentence that is either true or false.

Definition: A *proposition* is a claim that requires a proof.

Definition: A *theorem* is a strong proposition.

Definition: A *lemma* is a weak proposition.

Definition: A *corollary* follows immediately from a proposition.

Definition: An *axiom* is a given truth.

Example: Axiom: The square of a real number is nonnegative.

Example: Axiom: The sum of two even numbers is even. (You could prove this however if you wanted)

Note: In general, axioms are statements that a fellow typical math 135 student should know before entering this class.

Instructor's Comments: This is the 20 minute mark

Example: Show that for $\theta \in \mathbb{R}$, $\sin(3\theta) = 3\sin(\theta) - 4\sin^3(\theta)$.

Note: $\in$ means 'in; or 'belongs to' and $\mathbb{R}$ is the set of real numbers.

Proof: Recall these three axioms hold for all $x, y \in \mathbb{R}$:

1) $\sin^2(x) + \cos^2(x) = 1$

2) $\sin(x \pm y) = \sin(x)\cos(y) \pm \sin(y)\cos(x)$

3) $\cos(x \pm y) = \cos(x)\cos(y) \mp \sin(x)\sin(y)$

To prove equalities, we do left hand side to right hand side proofs (or vice versa). We can also meet in the middle and do half starting with the left hand side and half starting with the right hand side.

$$
\begin{aligned}
\text{LHS} &= \sin(3\theta) \\
&= \sin(2\theta + \theta) \\
&= \sin(2\theta)\cos(\theta) + \sin(\theta)\cos(2\theta) && \text{Use identity 2) with } x = 2\theta \text{ and } y = \theta \\
&= (2\sin(\theta)\cos(\theta))\cos(\theta) + \sin(\theta)(\cos^2(\theta) - \sin^2(\theta)) && \text{Use identity 2) and 3) with } x = y = \theta \\
&= 3\sin(\theta)\cos^2(\theta) - \sin^3(\theta)) \\
&= 3\sin(\theta)(1 - \sin^2(\theta)) - \sin^3(\theta)) && \text{Use identity 1) with } x = \theta \\
&= 3\sin(\theta) - 4\sin^3(\theta) \\
&= \text{RHS}
\end{aligned}
$$

Note: Make sure to identify the uses of trigonometric identities above. Be explicit.

Instructor's Comments: This is the 30-33 minute mark

In what follows, we will discuss good and bad proofs of Stewart's Theorem. Try to prove the theorem yourself.

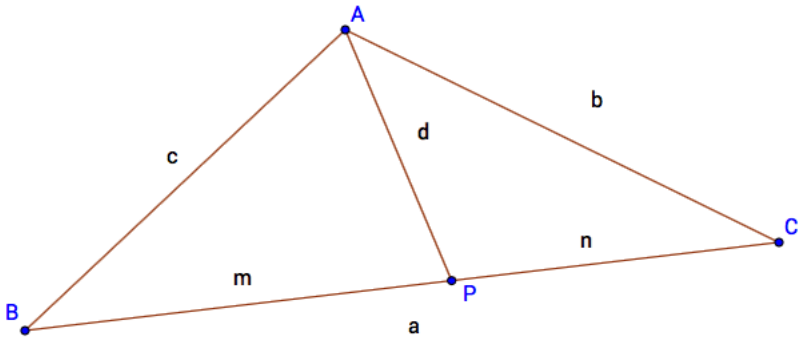
Instructor's Comments: This is the 38 minute mark

Then analyze the proofs for improvement.

Instructor's Comments: This will take you to the 46 minute mark

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 A**

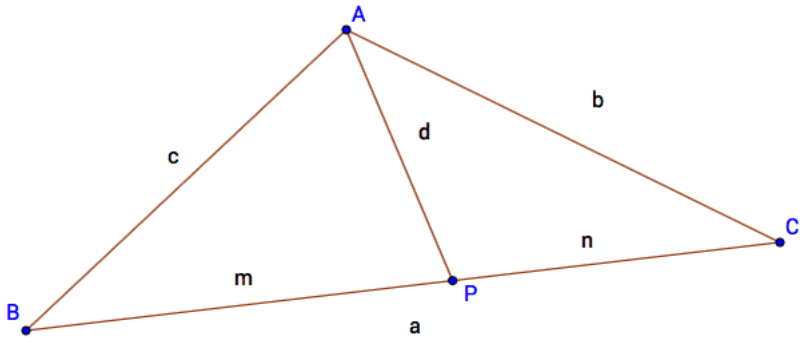
$$c^2 = m^2 + d^2 - 2md\cos\theta$$
$$b^2 = n^2 + d^2 - 2nd\cos\theta'$$
$$b^2 = n^2 + d^2 + 2nd\cos\theta$$
$$\frac{m^2 - c^2 + d^2}{-2md} = \frac{b^2 - n^2 - d^2}{2nd}$$
$$nc^2 - nm^2 - nd^2 = -mb^2 + mn^2 + md^2$$
$$nc^2 - mb^2 = mn^2 + md^2 + nm^2 + nd^2$$
$$cnc + bmb = nm(n + m) + d^2(m + n)$$
$$cnc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

■

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

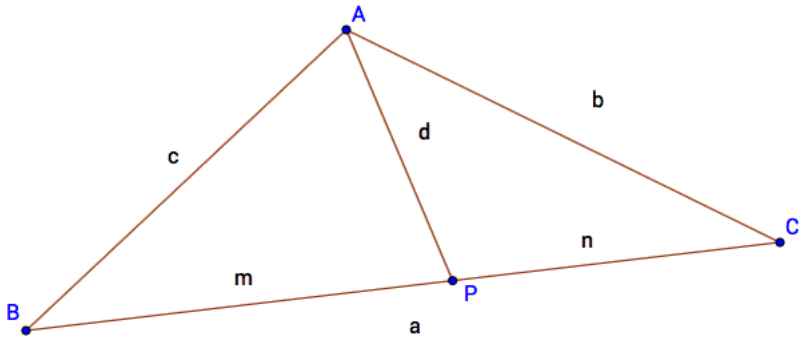
$$nma + d^2a = mb^2 + nc^2.$$

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 $dad + man = bmb + cnc$.



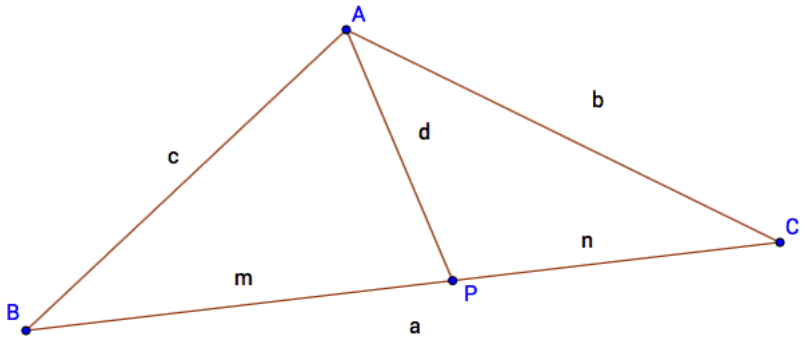
Proof. **Proof C**

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.

Instructor's Comments: This concludes up to the 46-48 minute mark

Handout or Document Camera or Class Exercise

Find the flaw in the following arguments:

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

$$\begin{aligned} a &= b \\ a^2 &= ab \\ a^2 - b^2 &= ab - b^2 \\ (a-b)(a+b) &= b(a-b) \\ a+b &= b \\ b+b &= b \\ 2b &= b \\ 2 &= 1 \end{aligned}$$

ERROR: division by 0 since $a = b$

Instructor's Comments: This is the end of lecture 2. Begin Lecture 3 with the next two examples.

(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 $x \in \mathbb{R}$,

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

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.

Instructor's Comments: This is the 20 minute mark

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

Instructor's Comments: This is the 26 minute mark

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 $2 \neq 2$

Solution: In order: True, False, True, True, False, True, False, True.
Note: For the last one above, the order of operations for logical operators (mathematically) is $\neg$, $\wedge$, $\vee$. If you change this order, the last bullet becomes false. This is not required knowledge in MATH 135 but you should make a note. Further, this is not consistent across programming languages.

Instructor's Comments: This is the 32 minute mark. It is possible to move this to the end of the lecture near the other similar handout if you want to avoid swapping back and forth from projector to notes.

Definition: The symbol $\equiv$ in logic means "logically equivalent", that is, in a truth table, the LHS and RHS are equivalent (share the same truth values for all possibilities; share the same truth values in columns, etc.). **Example:** Show that $\neg(\neg A) \equiv A$.
Proof:

A	$\neg A$	$\neg(\neg A)$
T	F	T
F	T	F

Since the first and last columns are equal, $A =\equiv \neg(\neg A)$.

Note: It is important to have a concluding statement like above. Make sure the reader knows why you know you have proven your statement.
Theorem: De Morgan's Law (DML)

$$\neg(A \vee B) \equiv \neg A \wedge \neg B$$
$$\neg(A \wedge B) \equiv \neg A \vee \neg B$$

We prove only the first. The second is left as an exercise.

A	B	$A \vee B$	$\neg(A \vee B)$	$\neg A$	$\neg B$	$\neg A \wedge \neg B$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Since the fourth and the last columns are equal, we have that $\neg(A \vee B) \equiv \neg A \wedge \neg B$ as required. ■

Instructor's Comments: It is worth noting that this is the first time an acronym is used. I am not certain if this acronym is in the textbook. This would be a good time to emphasize when using a theorem or a result, you should use the acronym or name.

Example: For Homework, prove that $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$.

Instructor's Comments: This is the 40 minute mark

Definition: Implication $(A \Rightarrow B)$

A	B	$A \Rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

In $A \Rightarrow B$, we call A the *hypothesis* and B the *conclusion*.

Note: Notice that if the hypothesis is false, the implication is always evaluated as true. Similarly, if the conclusion is true, the implication is always evaluated as true.

Note: To **prove** $A \Rightarrow B$, we **assume** A is true and then show that B is true.

Note: To **use** $A \Rightarrow B$, we **prove** A is true and then use B as true.

Proposition: Let A and B be statements. Then $A \Rightarrow B \equiv \neg A \vee B$.

Proof:

A	B	$A \Rightarrow B$	$\neg A$	$\neg A \vee B$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Since the third and fifth columns are equal, we see that $A \Rightarrow B \equiv \neg A \vee B$. ■

Handout or Document Camera or Class Exercise

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 $1 + 1 = 3$

Solution: True, False, True, True, True.

Instructor's Comments: This is the 50 minute mark

Lecture 4

Handout or Document Camera or Class Exercise

Instructor's Comments: Clicker Questions to start every 4th lecture.

Suppose A, B and C are all true statements.

The compound statement $(\neg A) \vee (B \wedge \neg C)$ is

A) True

B) False

Solution: The answer is False.

Instructor's Comments: This should take about 5 minutes. For all clicker questions, if the results are poor - get them to talk to each other and repoll.

Recall:

Proposition: Let A and B be statements. Then $A \Rightarrow B \equiv \neg A \vee B$.

Proposition: Let A and B be statements. Then $\neg(A \Rightarrow B) \equiv A \wedge \neg B$. Reworded, the negation of an implication is the hypothesis and the negation of the conclusion.

Proof:

$$\begin{aligned} \neg(A \Rightarrow B) &\equiv \neg(\neg A \vee B) && \text{By the above proposition} \\ &\equiv \neg(\neg A) \wedge \neg B && \text{De Morgan's Law} \\ &\equiv A \wedge \neg B && \text{By proposition from class} \end{aligned}$$

This completes the proof. ■

Instructor's Comments: This is the 10 minute mark. Note it is important to do the negation of implication with them.

Definition: Denote the set of integers by $\mathbb{Z}$.

Note: We use $\mathbb{Z}$ since this is the first letter of the word integer... in German! (Zählen)

Definition: Let $m, n \in \mathbb{Z}$. We say that m divides n and write $m \mid n$ if (and only if) there exists a $k \in \mathbb{Z}$ such that $mk = n$. Otherwise, we write $m \nmid n$, that is, when there is no integer k satisfying $mk = n$.

Note: The "(and only if)" part will be explained in a few lectures.

Instructor's Comments: I tell my students that definitions in mathematics should be if and only if however mathematicians are sloppy and do not do this in practice.

Example:

(i) $3 \mid 6$

(ii) $2 \mid 2$

(iii) $7 \mid 49$

(iv) $3 \mid -27$

(v) $6 \nmid 8$

(vi) $55 \mid 0$

(vii) $0 \mid 0$

(viii) $0 \nmid 3$

Instructor's Comments: This is the 17 minute mark

Example: Does $\pi \mid 3\pi$? This question doesn't make sense since in the definition of $\mid$, we required both m and n to be integers (there are ways to extend the definition but here we're restricting ourselves to talk only about integers when we use $\mid$).

Example: (Direct Proof Example) Prove $n \in \mathbb{Z} \wedge 14 \mid n \Rightarrow 7 \mid n$.

Proof: Let $n \in \mathbb{Z}$ and suppose that $14 \mid n$. Then $\exists k \in \mathbb{Z}$ s.t. $114k = n$. Then $(7 \cdot 2)k = n$. By associativity, $7(2k) = n$. Since $2k \in \mathbb{Z}$, we have that $7 \mid n$.

Note: The symbol $\exists$ means "there exists". the letters s.t. mean " such that".

Instructor's Comments: This is the 30 minute mark. It is not necessary to mention associativity above but I'll introduce rings at some point and so this seems like a good opportunity to remind students of what things they can take as axioms.

Recall: An integer n is

(i) Even if $2 \mid n$

(ii) Odd if $2 \mid (n-1)$.

Proposition: Let $n \in \mathbb{Z}$. Suppose that 2^{2n} is an odd integer. Show that 2^{-2n} is an odd integer.

Proof: Note that the hypothesis is only true when $n = 0$. If $n < 0$, then 2^{2n} is not an integer. If $n > 0$ then $2^{2n} = 2 \cdot 2^{2n-1}$ and since $2n - 1 > 0$, we see that 2^{2n} is even. Hence $n = 0$ and thus $2^{2n} = 1 = 2^{-2n}$. Thus 2^{-2n} is an odd integer. ■

Note: Ask yourself when is the hypothesis true. Then consider that/those case(s). Breaking up into cases is a great way to prove statements. Sometimes breaking a statement into even and odd, or positive and negative are great strategies.

Instructor's Comments: This is the 40 minute mark. Ask the students to attempt to give you a good definition of prime. This is a good exercise for students to make precise definitions.

Definition: An integer p is said to be *prime* if (and only if) $p > 1$ and its only positive divisors are 1 and p.

Example: Show that p and $p + 1$ are prime only when $p = 2$.

Instructor's Comments: Can do this example if you have time. Otherwise it's fine to leave it as an exercise

Proposition: Bounds by Divisibility (BBD).

$$a \mid b \wedge b \neq 0 \Rightarrow |a| \leq |b|$$

Proof: Let $a, b \in \mathbb{Z}$ such that $a \mid b$ and $b \neq 0$. Then $\exists k \in \mathbb{Z}$ such that $ak = b$. Since $b \neq 0$, we know that $k \neq 0$. Thus, $|a| \leq |a||k| = |ak| = |b|$ as required. ■

Instructor's Comments: This is probably the 50 minute mark. If you have time, state TD and DIC below.

Proposition: Transitivity of Divisibility (TD)

$$a \mid b \wedge b \mid c \Rightarrow a \mid c$$

Proof: There exists a $k \in \mathbb{Z}$ such that $ak = b$. There exists an $\ell \in \mathbb{Z}$ such that $b\ell = c$. This implies that $(ak)\ell = c$ and hence $a(k\ell) = c$. Since $k\ell \in \mathbb{Z}$, we have that $a \mid c$. ■

Proposition: Divisibility of Integer Combinations (DIC). Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$. Then for any $x, y \in \mathbb{Z}$, we have $a \mid (bx + cy)$.

A	B	$A \Leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

Note: Definitions in mathematics should (almost) always be if and only if definitions. Mathematicians generally are sloppy and don't do this. We will try to be careful in this course but you have been warned for other courses.

Exercise: Show that $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$

Example: In ΔABC, show that $b = c\cos A$ if and only if $\angle C = \frac{\pi}{2}$.

Proof: Suppose that $b = c\cos A$. By the Cosine Law,

$$\begin{aligned} a^2 &= b^2 + c^2 - 2bc\cos A \\ a^2 &= b^2 + c^2 - 2bb \\ a^2 &= c^2 - b^2 \\ a^2 + b^2 &= c^2 \end{aligned}$$

Is the converse of the Pythagorean Theorem true? Let's find out! Using the cosine law again,

$$\begin{aligned} c^2 &= a^2 + b^2 - 2ab\cos C \\ c^2 &= c^2 - 2ab\cos C \\ 0 &= -2ab\cos C \end{aligned}$$

Therefore, $\cos C = 0$ since $0 < \angle C < \pi$, we see that $\angle C = \pi/2$.

Now we prove the converse. Suppose that $\angle C = \pi/2$. Then ΔABC is a right angled triangle! Hence, $\cos A = \frac{b}{c}$ and thus $c\cos A = b$ as required. ■

Instructor's Comments: This should be the 35 minute mark. Emphasize proving the converse in iff proofs.

Handout or Document Camera or Class Exercise

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

Instructor's Comments: Give 5 minutes to try it and 5 minutes to take it up.

Proof: Suppose first that $\frac{x+y}{2} = \sqrt{xy}$. Then

$$\begin{aligned} \frac{x+y}{2} &= \sqrt{xy} \\ x+y &= 2\sqrt{xy} \\ (x+y)^2 &= (2\sqrt{xy})^2 \\ x^2+2xy+y^2 &= 4xy \\ x^2-2xy+y^2 &= 0 \\ (x-y)^2 &= 0. \end{aligned}$$

Therefore, $x - y = 0$ and thus $x = y$. Now, suppose first that $x = y$. Then

$$\text{LHS} = \frac{x+y}{2} = \frac{y+y}{2} = \frac{2y}{2} = y$$

and

$$\text{RHS} = \sqrt{xy} = \sqrt{y^2} = y$$

with the last equality holding since $y \geq 0$. Therefore, $\frac{x+y}{2} = \sqrt{xy}$.

Instructor's Comments: This is the 45 minute mark.

Definition: A *set* is a collection of elements.

Example:

(i) $\mathbb{Z} = \{... -2, -1, 0, 1, 2, ...\}$

(ii) $\mathbb{N} = \{1, 2, ...\}$

(iii) $\mathbb{R}$

(iv) $\mathbb{Q} = \{a/b \in \mathbb{R} : a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge b \neq 0\}$ (We call $\mathbb{R}$ the *universe of discourse*.

(v) $\{5, A\}$

(vi) $S = \{\blacksquare, 2, \{1, 2\}\}$

Note: For Math 135, the natural numbers begin with the element 1. (Some textbooks or courses start with 0).

Note: $x \in S$ means x in S (or x belongs to S) and $x \notin S$ means x not in S.

Instructor's Comments: If you have time here do these, otherwise start the next lecture with these two points.

Note: $\{\}$ and $\emptyset$ are the empty set, a set with no elements.

Note: $\{\emptyset\}$ is NOT the empty set. It is a set with one element, the element that is the empty set.

Handout or Document Camera or Class Exercise

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.

Instructor's Comments: 5 minutes to try on their own and 5 to take up

Solution:

(i) $\{6, 8, 10, 12, 14\}$ or $\{n \in \mathbb{N} : 5 \leq n \leq 14 \wedge 2 \mid n\}$

(ii) $\{(2k+1)^2 : k \in \mathbb{Z}\}$ (or $\mathbb{N}$ overlap doesn't matter!)

(iii) $\{(a, b, c) : a, b, c \in \mathbb{N} \wedge a < b + c \wedge b < a + c \wedge c < a + b\}$

(iv) $\{(x, y) : x, y \in \mathbb{R} \wedge x^2 + y^2 = 8^2\}$

Instructor's Comments: This is the 17 minute mark

Set Operations. Let S and T be sets. Define

(i) $\#S$ or $|S|$. Size of the set S.

(ii) $S \cup T = \{x : x \in S \vee x \in T\}$ (Union)

(iii) $S \cap T = \{x : x \in S \wedge x \in T\}$ (Intersection)

(iv) $S - T = \{x \in S : x \notin T\}$ (Set difference)

(v) $\bar{S}$ or S^c (with respect to universe U) the complement of S, that is

$$S^c = \{x \in U : x \notin S\} = U - S$$

(vi) $S \times T = \{(x, y) : x \in S \wedge y \in T\}$ (Cartesian Product)

Example: $(1, 2) \in \mathbb{Z} \times \mathbb{Z}$, $(2, 1) \in \mathbb{Z} \times \mathbb{Z}$, BUT $(1, 2) \neq (2, 1)$.

Note: $\mathbb{Z} \times \mathbb{Z}$ and $\{(n, n) : n \in \mathbb{Z}\}$ are different sets!!!

Example:

$$\mathbb{Z} = \{m \in \mathbb{Z} : 2 \mid m\} \cup \{2k + 1 : k \in \mathbb{Z}\}$$
$$\emptyset = \{m \in \mathbb{Z} : 2 \mid m\} \cap \{2k + 1 : k \in \mathbb{Z}\}$$

Instructor's Comments: This is the 30-33 minute mark

Definition: Let S and T be sets. Then

(i) $S \subseteq T$: S is a subset of T. Every element of S is an element of T.

(ii) $S \subsetneq T$: S is a proper/strict subset of T. Every element of S is an element of T and some element of T is not in S.

(iii) $S \supseteq T$: S contains T. Every element of T is an element of S.

(iv) $S \supsetneq T$: S properly/strictly contains T. Every element of T is an element of S and some element of S is not in T.

Definition: $S = T$ means $S \subseteq T$ and $T \subseteq S$.

Example: $\{1, 2\} = \{2, 1\}$

Example: Prove $\{n \in \mathbb{N} : 4 \mid (n + 1)\} \subseteq \{2k + 1 : k \in \mathbb{Z}\}$

Proof: Let $m \in \{n \in \mathbb{N} : 4 \mid (n + 1)\}$. Then $4 \mid (m + 1)$. Thus, $\exists \ell \in \mathbb{Z}$ such that $4\ell = m + 1$. Now

$$m = 2(2\ell) - 1 = 2(2\ell) - 2 + 2 - 1 = 2(2\ell - 1) + 1.$$

Hence $m \in \{2k + 1 : k \in \mathbb{Z}\}$. ■

Instructor's Comments: This is the 40-43 minute mark. You might run out of time in the next example. Carry forward to Lecture 7 as need be.

Example: Show $S = T$ if and only if $S \cap T = S \cup T$.

Proof: Suppose $S = T$. To show $S \cap T = S \cup T$ we need to show that $S \cap T \subseteq S \cup T$ and that $S \cap T \supseteq S \cup T$

First suppose that $x \in S \cap T$. Then $x \in S$ and $x \in T$. Hence $x \in S \cup T$.

Next, suppose that $x \in S \cup T$. Then $x \in S$ or $x \in T$. Since $S = T$ we have in either case that $x \in S$ and $x \in T$. Thus $x \in S \cap T$. This shows that $S \cap T = S \cup T$ and completes the forward direction.

Now assume that $S \cap T = S \cup T$. We want to show that $S = T$ which we do by showing that $S \subseteq T$ and $T \subseteq S$.

First, suppose that $x \in S$. Then $x \in S \cup T = S \cap T$. Hence $x \in T$.

Next, suppose that $x \in T$. Then $x \in S \cup T = S \cap T$. Hence $x \in S$. Therefore, $S = T$.
■

Instructor's Comments: The last two points give a good learning moment to explain when the word 'similarly' can be used. This is the 50 minute mark.

Lecture 7

Quantified Statements

(i) For every natural number n, $2n^2 + 11n + 15$ is composite.

(ii) There is an integer k such that $6 = 3k$.

Symbolically, we write

(i) $\forall n \in \mathbb{N}$, $2n^2 + 11n + 15$ is composite.

(ii) $\exists k \in \mathbb{Z}$ such that $6 = 3k$.

We call $\forall$ and $\exists$ quantifiers, n and k variables, $\mathbb{N}$ and $\mathbb{Z}$ domains and the rest are called an open sentence (usually involving the variable(s)).

Note: $\forall x \in S\, P(x)$ means for all x in S, statment $P(x)$ holds. This is equivalent to $x \in S \Rightarrow P(x)$.

Proof: (of number 1 above) Let n be an arbitrary natural number. Then factoring gives $2n^2 + 11n + 15 = (2n + 5)(n + 3)$. Since $2n + 5 > 1$ and $n + 3 > 1$, we have $2n^2 + 11n + 15$ is composite.

Proof: (of number 2 above) Since $3 \cdot 2 = 6$, we see that $k = 2$ satisfies the given statement.

Example: $S \subseteq T \equiv \forall x \in S\, x \in T$

Instructor's Comments: This is the 7 minute mark

Handout or Document Camera or Class Exercise

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

Proof: When $x = 2$, note that $\frac{2^2+3(2)-3}{2(2)+3} = \frac{7}{7} = 1$. ■

Note: : The discovery of this proof is perhaps what is more interesting:

$$\frac{x^2+3x-3}{2x+3} = 1 \quad \Leftrightarrow \quad x^2+3x-3 = 2x+3 \quad \Leftrightarrow \quad x^2+x-6 = 0$$

and the last equation factors as $(x-2)(x+3) = 0$ and hence $x = 2$.

Instructor's Comments: This is the 17 minute mark

Note: : Vacuously true statements $\forall x \in \emptyset, P(x)$. Since there is no element in the empty set, we define this statement to always be true as a matter of convention.

Example: Let $a, b, c \in \mathbb{Z}$. If $\forall x \in \mathbb{Z}$, $a \mid (bx + c)$ then $a \mid (b + c)$.

Proof: Assume $\forall x \in \mathbb{Z}$, $a \mid (bx + c)$. Then, for example, when $x = 1$, we see that $a \mid (b(1) + c)$. Thus $a \mid (b + c)$.

Instructor's Comments: Note: If you're running short on time, this next example can be omitted

Example: $\exists m \in \mathbb{Z}$ such that $\frac{m-7}{2m+4} = 5$.

Proof: When $m = 3$, note that $\frac{m-7}{2m+4} = \frac{-3-7}{2(-3)+4} = \frac{-10}{-2} = 5$

Instructor's Comments: This should be the 26-30 minute mark

Handout or Document Camera or Class Exercise

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

Instructor's Comments: For the next two pages, you should give students say 5 minutes each (maybe more for the second handout) and then take them up as a class for 5 minutes each

Proof: Let $x \in \mathbb{R}$ be arbitrary. Then

$$\begin{aligned} x^2 + 4x + 7 &= x^2 + 4x + 4 - 4 + 7 \\ &= (x+2)^2 + 3 \\ &> 0 \end{aligned}$$

Handout or Document Camera or Class Exercise

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.

Solution:

(i) $\forall n \in \mathbb{N}, 2n^2 + 11n + 15$ is not prime.

(ii) $\forall n \in \mathbb{N}, 2n^2 + 11n + 15$ is composite.

(iii) $\exists m \in \mathbb{Z}, \frac{m-7}{2m+4} = 5$.

(iv) $\exists m \in \mathbb{Z}, \frac{m-7}{2m+4} = 5$.

Instructor's Comments: This should be about the 46 minute mark

Note: : Domain is important!

Let $P(x)$ be the statement $x^2 = 2$ and let $S = \{\sqrt{2}, -\sqrt{2}\}$. Which of the following are true?

(i) $\exists x \in \mathbb{Z}, P(x)$

(ii) $\forall x \in \mathbb{Z}, P(x)$

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

(iv) $\forall x \in \mathbb{R}, P(x)$

(v) $\exists x \in S, P(x)$

(vi) $\forall x \in S, P(x)$

Solution:

(i) False

(ii) False

(iii) True

(iv) False

(v) True

(vi) True

Instructor's Comments: This is the end of the lecture.

Lecture 8

Handout or Document Camera or Class Exercise

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 $8 \mid (2k+4)$.

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

Instructor's Comments: This is the 5 minute mark

Handout or Document Camera or Class Exercise

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.

Instructor's Comments: This is the 10-13 minute mark

Negating Quantifiers Example: Negate the following:

(i) Everybody in this room was born before 2010.

Solution: Somebody in this room was not born before 2010.

(ii) Someone in this room was born before 1990

Solution: Everyone in this room was born after 1990.

(iii) $\forall x \in \mathbb{R}, |x| < 5$

Solution: $\neg(\forall x \in \mathbb{R}, |x| < 5) \equiv \exists x \in \mathbb{R}, |x| \geq 5$

(iv) $\exists x \in \mathbb{R}, |x| \leq 5$

Solution: $\neg(\exists x \in \mathbb{R}, |x| \leq 5) \equiv \forall x \in \mathbb{R}, |x| > 5$

Instructor's Comments: Let them validate the truth of the above statements. This could take you to the 20 minute mark easily

Note: A proof that a statement is false is called a disproof.

Example: Prove or disprove: Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ then $a \mid b$ or $a \mid c$.

Solution: This is false! A counter example is given by $a = 6$, $b = 2$ and $c = 3$. Then $a \mid bc$ BUT $6 \nmid 2$ and $6 \nmid 3$.

Note: It turns out that this is true if you require additionally that a is prime. This is called Euclid's Lemma. We'll see a proof of this in 5 weeks. It is actually very nontrivial to prove.

Instructor's Comments: Get them to think about the prime condition. The proof of this requires GCDs in the prime case to the best of my knowledge. This is the 27 minute mark.

Handout or Document Camera or Class Exercise

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

Solution:

(i) False (Choose $x = y = 0$)

(ii) True (Choose $x = 1$ and $y = 0$)

(iii) True.

Proof: Let $x \in \mathbb{R}$ be arbitrary. then choose $y = \sqrt[3]{x^3 - 1}$. Then

$$x^3 - y^3 = x^3 - (\sqrt[3]{x^3 - 1})^3 = x^3 - (x^3 - 1) = 1$$

(iv) False. Idea: Negate and show the negation is true!

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

Proof: Let $x \in \mathbb{R}$ be arbitrary. Take $y = x$. Then $x^3 - y^3 = x^3 - x^3 = 0 \neq 1$.

Instructor's Comments: This is the 40 minute mark

Handout or Document Camera or Class Exercise

List all elements of the set:

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

Solution: The first set is the set of all primes. The second set is the set of all divisors of 42, namely

$$\{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}.$$

The intersection is therefore $\{2, 3, 7\}$.

Check out `http://www.cemc.uwaterloo.ca/~cbruni/Math135Resources.php` for symbol cheat sheets and theorem cheat sheets and other goodies!

Instructor's Comments: End of class

Lecture 9

Handout or Document Camera or Class Exercise

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.

Solution:

(i) $\forall m, n \in \mathbb{Z}, (15m + 6n \neq 100)$

(ii) $\forall m, n \in \mathbb{Z}, ((3 \mid (m+n) \wedge 3 \mid (m-n)) \Rightarrow 3 \mid m \wedge 3 \mid n)$

Instructor's Comments: This is the 10 minute mark

Handout or Document Camera or Class Exercise

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

Solution:

(i) If m is an even integer, then $7m^2 + 4$ is even.

(ii) There is no greatest integer. (Alternatively, for every integer, there exists a greater integer).

Instructor's Comments: This is the 20 minute mark

Contrapositive

Note: Proofs are not always easy to discover. Sometimes you can convert a given problem to an easier equivalent problem.

Example: $7 \nmid n \Rightarrow 14 \nmid n \equiv 14 \mid n \Rightarrow 7 \mid n$

Definition: The *contrapositive* of $H \Rightarrow C$ is $\neg C \Rightarrow \neg H$.

Note: $H \Rightarrow C \equiv \neg C \Rightarrow \neg H$. This follows since

$$\begin{aligned} H \Rightarrow C &\equiv \neg H \vee C \\ &\equiv C \vee \neg H \\ &\equiv \neg(\neg C) \vee \neg H \\ &\equiv \neg C \Rightarrow \neg H \end{aligned}$$

or by using a Truth table

H	C	$H \Rightarrow C$	$\neg C$	$\neg H$	$\neg C \Rightarrow \neg H$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Since the third and sixth columns are equal, their headings are logically equivalent.

Instructor's Comments: This is the 32-37 minute mark

Example: Let $x \in \mathbb{R}$. Prove $x^3 - 5x^2 + 3x \neq 15 \Rightarrow x \neq 5$.

Proof: We prove the contrapositive. Let $x = 5$. Then

$$\begin{aligned} x^3 - 5x^2 + 3x &= (5)^3 - 5(5)^2 + 3(5) \\ &= 5^3 - 5^3 + 15 \\ &= 15. \end{aligned}$$

■

Example: Suppose $a, b \in \mathbb{R}$ and $ab \in \mathbb{R} - \mathbb{Q}$ (the set of irrational numbers). Show either $a \in \mathbb{R} - \mathbb{Q}$ or $b \in \mathbb{R} - \mathbb{Q}$.

Proof: Proceed by the contrapositive. Suppose that a is rational and b is rational. Then $\exists k, \ell, m, n \in \mathbb{Z}$ such that $a = \frac{k}{\ell}$ and $b = \frac{m}{n}$ with $\ell, n \neq 0$. Then

$$ab = \tfrac{km}{\ell n} \in \mathbb{Q}$$

as required. ■

Instructor's Comments: This is the 50 minute mark.

Lecture 10

Handout or Document Camera or Class Exercise

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

Proof: We prove the contrapositive. Suppose that $x \geq 1.1 > 1$. Then

$$\begin{aligned} x^3 + 7x^2 &\geq (1.1)^3 + 7(1.1)^2 \\ &= \left(\frac{11}{10}\right)^3 + 7\left(\frac{11}{10}\right)^2 \\ &= \frac{1331}{1000} + 7\left(\frac{121}{100}\right) \qquad = \frac{1331 + 8470}{1000} \\ &= \frac{9801}{1000} \\ &\geq 9 \end{aligned}$$

as required. ■

Instructor's Comments: This is the 10 minute mark

Types of Implications

Let A, B, C be statements.

(i) $(A \wedge B) \Rightarrow C$ These we have seen in say Divisibility of Integer Combinations or Bounds by Divisibility.

(ii) $A \Rightarrow (B \wedge C)$.

Example: Let S, T, U be sets. If $(S \cup T) \subseteq U$, then $S \subseteq U$ and $T \subseteq U$.

Proof: Suppose $S \cup T \subseteq U$. If $x \in S$, then $x \in S \cup T \subseteq U$. Thus $x \in U$. Thus, $S \subseteq U$. By symmetry (or similarly), $T \subseteq U$. ■

Instructor's Comments: Here you can make note of the use of the word 'similarly'. It should be used sparingly and only when the argument is truly identical.

(iii) $(A \vee B) \Rightarrow C$

Example: $(x = 1 \vee y = 2) \Rightarrow x^2y + y - 2x^2 + 4x - 2xy = 2$

Proof: Assume that $(x = 1 \vee y = 2)$. Then one of these two values is true. If $x = 1$, then

$$\begin{aligned} \text{LHS} &= x^2y + y - 2x^2 + 4x - 2xy \\ &= (1)^2y + y - 2(1)^2 + 4(1) - 2(1)y \\ &= y + y - 2 + 4 - 2y \\ &= 2 \\ &= \text{RHS}. \end{aligned}$$

If instead $y = 2$, then

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

completing the proof. ■

(iv) $A \Rightarrow (B \vee C)$. (Elimination)

Example: If $x^2 - 7x + 12 \geq 0$ then $x \leq 3 \vee x \geq 4$.

Proof: Suppose $x^2 - 7x + 12 \geq 0$ and $x > 3$. Then $0 \leq x^2 - 7x + 12 = (x-3)(x-4)$. Now, $x - 3 > 0$ and so we must have that $x - 4 \geq 0$. Hence $x \geq 4$.

Instructor's Comments: This is the 25-30 minute mark

Handout or Document Camera or Class Exercise

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

A) -3

B) 49

C) 1000000

D) 1500

Instructor's Comments: Argue that many answers are ridiculous and so only the plausible answer remains. Change the second answer to (current year - 1967). You could also introduce contradiction by using a sudoku board which can be fun.

Proof by contradiction

Let S be a statement. Then $S \wedge \neg S$ is false.

Instructor's Comments: Mention we sometimes use # to denote a contradiction has been reached.

Example: There is no largest integer.

Proof: Assume towards a contradiction that M_0 is the largest integer. Then, since $M_0 < M_0 + 1$ and $M_0 + 1 \in \mathbb{Z}$, we have contradicted the definition of M_0. Thus, no largest integer exists. ■

Instructor's Comments: This is the 32-37 minute mark

Handout or Document Camera or Class Exercise

Instructor's Comments: The following is an example of reading proofs and seeing the difference between the direct proofs and proofs by contradiction.

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.

Instructor's Comments: This is the 40 minute mark.

Instructor's Comments: It should be noted that the Well Ordering Principle is not officially in the Math 135 curriculum. Since it is an easier to understand form of Mathematical Induction, I've chosen to include it.

Axiom Well Ordering Principle (WOP). Every subset of the natural numbers that is nonempty contains a least element.

Handout or Document Camera or Class Exercise

Instructor's Comments: It's conceivable that you might want to write out the first proof and then display the other two proofs. Feel free to ignore these proofs as well. I do however recommend the first one.

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.

Instructor's Comments: If you do all three proofs, notice that the simple proof and the infinite descent proofs are similar.

Lecture 11

Uniqueness

Definition: $\exists!$ means "There exists a unique".

Note: To prove uniqueness, we can do one of the following:

(i) Assume $\exists x, y \in S$ such that $P(x) \wedge P(y)$ is true and show $x = y$.

(ii) Argue by assuming that $\exists x, y \in S$ are distinct such that $P(x) \wedge P(y)$, then derive a contradiction.

To prove uniqueness and existence, we also need to show that $\exists x \in S$ such that $P(x)$ is true.

Example: Suppose $x \in \mathbb{R} - \mathbb{Z}$ and $m \in \mathbb{Z}$ such that $x < m < x + 1$. Show that m is unique.

Proof: Assume that $\exists m, n \in \mathbb{Z}$ such that

$$x < m < x + 1 \qquad \text{and} \qquad x < n < x + 1$$

Look at the value $m - n$. This value is largest when m is largest and n is smallest. Since $m < x + 1$ and $n > x$, we see that $m - n < 1$. Further, for this to be minimal, we could flip the roles of m and n above to see that $-1 < m - n$. Thus $-1 < m - n < 1$ and $m - n \in \mathbb{Z}$. Hence $m - n = 0$, that is $m = n$.

Handout or Document Camera or Class Exercise

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 $f(x) = y$

Instructor's Comments: Some things to note: This is the first time students will realize that in order to properly define a function, a function has a domain and codomain that are given. Note that the range is the set of all values the domain maps into. The codomain might actually be larger than the range. They have not seen this notation before so you'll be wise to explain to them that this is the same as $f(x) = x^2$.

Proof: Existence. For each $y \in (0, \infty)$, let $x = \sqrt{y}$. Then

$$f(x) = f(\sqrt{y}) = (\sqrt{y})^2 = y$$

Uniqueness. Suppose that there exists $a, b \in (0, \infty)$ such that

$$\begin{aligned} f(a) &= f(b) \\ a^2 &= b^2 \\ |a| &= |b| \end{aligned}$$

and since $a, b > 0$, we have that $a = b$. ■

Instructor's Comments: Use this as a lead in to Injections and Surjections. This is the 15 minute mark.

Injections and Surjections

Definition: Let S and T be sets. A function $f : S \to T$ is said to be

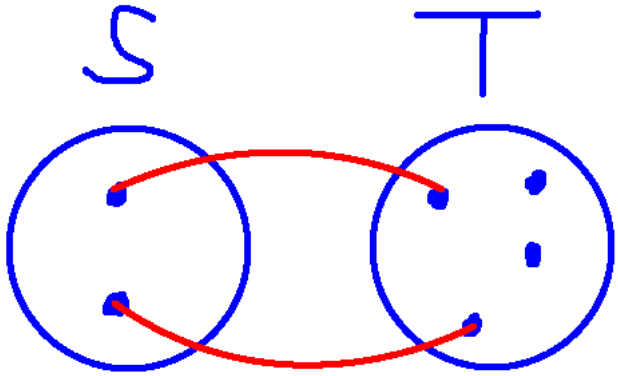
(i) Injective (or one to one or $1:1$) if and only if

$$\forall x, y \in S, f(x) = f(y) \Rightarrow x = y.$$

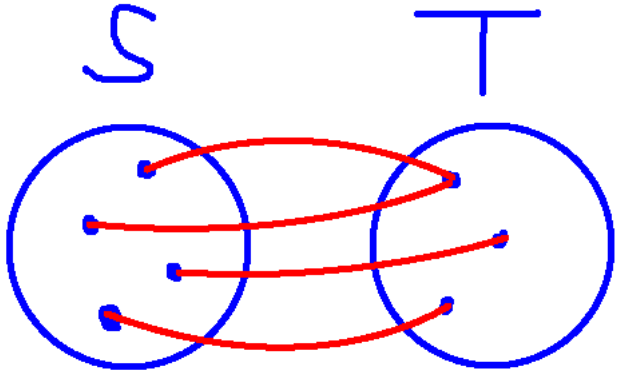
(ii) Surjective (or onto) if and only if

$$\forall y \in T \ \exists x \in S \text{ such that } f(x) = y$$

Example: A function that is one to one but not onto:



Example: A function that is onto but not one to one:



Example: Prove

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

is not injective.

Proof: Notice that

$$f(-1) = (-1)^2 = 1 = (1)^2 = f(1)$$

but $-1 \neq 1$. ■

Instructor's Comments: Emphasize that this is the negation of the definition above. Disproving a for all means finding a counter example.

Example: Prove

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto 2x^3 + 1 \end{aligned}$$

is one to one.

Proof: Let $x, y \in \mathbb{R}$ such that $f(x) = f(y)$. Then

$$\begin{aligned} 2x^3 + 1 &= 2y^3 + 1 \\ x^3 &= y^3 \\ \sqrt[3]{x^3} &= \sqrt[3]{y^3} \\ x &= y \end{aligned}$$

Thus f is injective. ■

Example: Prove

$$\begin{aligned} f : \mathbb{R} &\to (-\infty, 1) \\ x &\mapsto 1 - e^{-x} \end{aligned}$$

is onto.

Proof: We need to show that every $y \in (-\infty, 1)$ has some $x \in \mathbb{R}$ with $f(x) = y$.

Discovery:

$$\begin{aligned} 1 - e^{-x} &= y \\ e^{-x} &= 1 - y \\ -x &= \ln(1 - y) \\ x &= -\ln(1 - y) \end{aligned}$$

Formal proof: Take $x = -\ln(1 - y)$ for any $y \in (-\infty, 1)$. Notice that this is well defined since $\ln(1 - y)$ is defined on $(-\infty, 1)$. Then

$$\begin{aligned} f(x) &= 1 - e^{-x} \\ &= 1 - e^{-(-\ln(1-y))} \\ &= 1 - e^{\ln(1-y)} \\ &= 1 - (1 - y) \\ &= y \end{aligned}$$

Therefore, f is an onto function. ■

Instructor's Comments: This is the 35-40 minute mark.

Division Algorithm

This is just like grade school division. For example, $51/7$ can be written as:

$$51 = 7(7) + 2$$

where $a = 51$, $b = 7$, $q = 7$ and $r = 2$. Similarly, $-35/6$ can be written as

$$-35 = 6(-6) + 1$$

where $a = -35$, $b = 6$, $q = -6$, and $r = 1$.

Handout or Document Camera or Class Exercise

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 $r_1 < r_2$.

Instructor's Comments: Introduce the acronym WLOG. Explain that if two integers are not equal, then one must be bigger than the other and the proof is symmetric depending if $r_1 < r_2$ or $r_2 < r_1$

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

Instructor's Comments: Take the difference of the two a values. Given that $0 \leq r_1, r_2 < b$, the biggest value of $r_2 - r_1$ is b.

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

Instructor's Comments: This is a contradiction. Notice that we don't need $|b|$ as in (BBD) since $b \in \mathbb{N}$.

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 $q_1 = q_2$.

Instructor's Comments: This is the 50 minute mark. Note you could leave the division algorithm for extra reading if you'd like and replace it by an example with a negative number. If you have time, I'd recommend digesting the Division algorithm proof carefully. If you're really ahead try the following: Define a line to be the set of points (x, y) satisfying $y = mx + b$ for some $m, b \in \mathbb{R}$. Show that if two lines have distinct slopes (m values) and that they intersect, then this solution is unique.

Lecture 12

Handout or Document Camera or Class Exercise

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

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

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.

Solution: None of the above (Watch the inequality signs above!).

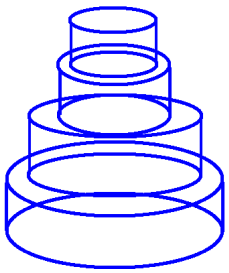
Instructor's Comments: This is the 5 minute mark. You will likely want to repoll the students (when I first gave this problem, many of my students got this wrong).

Instructor's Comments: This is a catch up lecture where if anything form the previous lectures took too long, then you can use this lecture to catch up. The only thing I would do in this lecture is show them sigma notation which I will do first and then give the class a lot of time to do practice problems.

Introduction to Summations

Example: Tower of Hanoi:

In this modified version of the Tower of Hanoi, we create a tower with levels where each level is a cylinder of height 1 and increasing radius begining with 1 and increasing by 1 at each level. Below is a level 4 Tower of Hanoi



Question: What is the volume of the 4 level Tower of Hanoi?

Solution:

$$\begin{aligned} V_{Tower} &= V_1 + V_2 + V_3 + V_4 \\ &= \pi(1)^2(1) + \pi(2)^2(1) + \pi(3)^2(1) + \pi(4)^2(1) \\ &= \pi + 4\pi + 9\pi + 16\pi \\ &= 30\pi \end{aligned}$$

Question: What about computing the volume of the 100 level Tower of Hanoi?

Solution:

$$\begin{aligned} V_{Tower} &= V_1 + V_2 + ... + V_{100} \\ &= \pi(1)^2(1) + \pi(2)^2(1) + ... + \pi(100)^2(1) \\ &= \pi + 4\pi + ... + 10000\pi \end{aligned}$$

Note: There are two concerns here. How do we evaluate this last sum? How to we write the above sum nicely and more formally without using dots?

Instructor's Comments: This is the 10 minute mark.

Sigma and Pi Notation

Definition: Let $\{a_1, ..., a_n\}$ be a sequence of n real numbers. We write

$$\sum_{i=1}^{n} a_i := a_1 + a_2 + ... + a_n.$$

We call i the index variable, 1 is the starting number, n is the upper bound. We can also write

$$\sum_{x \in S} x$$

to mean the sum of elements in S.

Instructor's Comments: Make sure you discuss the := symbol.

Similarly, we define

$$\prod_{i=1}^{n} a_i := a_1 a_2 ... a_n \qquad \prod_{x \in S} = \text{ Product of elements in S}$$

We make the following conventions when $j > k$ are integers (that is, the start index exceeds the end index)

$$\sum_{i=j}^{k} a_i = \sum_{x \in \emptyset} = 0$$

and further,

$$\prod_{i=j}^{k} a_i = \prod_{x \in \emptyset} = 1$$

Note: Sums are linear:

$$\text{For } c, j, k \in \mathbb{Z}, \sum_{i=j}^{k} (ca_i \pm b_i) = c \sum_{i=j}^{k} a_i \pm \sum_{i=j}^{k} b_i$$

Example:

(i) $\sum_{i=1}^{4} i^2 = (1)^2 + (2)^2 + (3)^2 + (4)^2 = 1 + 4 + 9 + 16 = 30$

(ii) $\prod_{i=1}^{4} i^2 = (1)^2(2)^2(3)^2(4)^2 = (1)(4)(9)(16) = 576$

(iii) $\sum_{i=1}^{3.5} i = 1 + 2 + 3 = 6$

(iv) For $k \in \mathbb{N}$ fixed, $\sum_{i=k}^{2k} 1/i = 1/k + 1/(k+1) + ... + 1/(2k)$.

(v) So we can write the 100 level tower of Hanoi volume as $\sum_{i=1}^{100} \pi i^2 = \pi \sum_{i=1}^{100} i^2$

Definition: We define the factorial notation for $n \geq 0$ an integer by $n! := \prod_{i=1}^{n} i$. Note $0! = 1$.

Example: $4! = (4)(3)(2)(1) = 24$.

Note: We will see next week how to compute the sum in our volume computation of the 100 level Tower of Hanoi.

Instructor's Comments: This is the 25-30 minute mark

Handout or Document Camera or Class Exercise

Instructor's Comments: I suggest letting students work on these and either getting them to write solutions on the board or at least telling you which ones they want to see solved.

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 $a \nmid c$.

Instructor's Comments: Hints in order

(i) Direct proof with cases

(ii) iff, contrapositive

(iii) contrapositive

(iv) contradiction

(v) factor

(vi) set inclusion

(vii) contrapositive and elimination.

Solution:

- Let $a, b \in \mathbb{R}$. Without loss of generality, suppose that $a \leq b$. Then $2\min\{a, b\} = 2a < a + b$. Hence $\min\{a, b\} \leq \frac{a+b}{2}$

- Let x be real. Then

$$\begin{aligned} x^2 - x > 0 &\Leftrightarrow x(x-1) > 0 \\ &\Leftrightarrow x > 0 \wedge x - 1 > 0 \text{ or } x < 0 \wedge x - 1 < 0 \\ &\Leftrightarrow x > 1 \text{ or } x < 0 \\ &\Leftrightarrow x \notin [0, 1]. \end{aligned}$$

- We proceed by the contrapositive. If $\frac{1}{r}$ is rational, say $\frac{1}{r} = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $b \neq 0$, then $r = \frac{b}{a} \in \mathbb{Q}$.

- Assume towards a contradiction that there exists integers p and q satisfying $p^2 - q^2 = 10$. Without loss of generality, we may assume that $p, q \geq 0$ since $p^2 = (-p)^2$ so if (p, q) is a solution, then all of $(\pm p, \pm q)$ are solutions. Factoring gives $(p-q)(p+q) = 10$. Since $p + q > 0$, we have that $p - q > 0$. Since $p - q < p + q$, we see that $p - q = 1$ and $p + q = 10$ or $p - q = 2$ and $p + q = 5$. Adding the two equalities gives $2p = 11$ and $2p = 7$, both of which are a contradiction since p is an integer.

  Instructor's Comments: The previous problem can also be solved by a parity argument.

- Isolating and factoring gives $x^2 + (y-1)^2 = 0$. Hence $x = 0$ and $y = 1$.

- Suppose that $x \in \overline{S \cap T}$. We are required to show that $x \in \overline{S} \cup \overline{T}$. By definition, $x \in U - (S \cap T)$ and hence $x \in U$ and $x \notin S \cap T$. Thus, if $x \in T$, then $x \notin S$ and so $x \in \overline{S}$. Otherwise, $x \notin T$ and hence $x \in \overline{T}$. Thus, $x \in \overline{S} \cup \overline{T}$.

- We prove the contrapositive. Suppose that $a \mid c$. Then we need to show that $a \mid b$ or $a \nmid (b+c)$. By elimination, we may assume that $a \mid (b+c)$ (otherwise $a \nmid (b+c)$ and the conclusion is true). Now, $a \mid c$ and $a \mid (b+c)$ and so by Divisibility of Integer Combinations, we have that $a \mid c(-1) + (b+c)(1)$ and hence $a \mid b$.

Lecture 13

Principle of Mathematical Induction (POMI)

Axiom: If sequence of statements $P(1)$, $P(2)$, ... satisfy

(i) $P(1)$ is true

(ii) For any $k \in \mathbb{N}$, if $P(k)$ is true then $P(k+1)$ is true

then $P(n)$ is true for all $n \in \mathbb{N}$.

Instructor's Comments: Here describe the domino analogy. Explain that you're creating a chain of implications $P(1) \Rightarrow P(2)$, $P(2) \Rightarrow P(3)$, and so on and you want the chain to begin.

In practice, these arguments proceed as follows:

(i) Prove the base case, that is, verify that $P(1)$ is true

(ii) Inductive hypothesis: Let $k \in \mathbb{N}$ be an arbitrary number. Assume that $P(k)$ is true.

(iii) Inductive conclusion. Deduce that $P(k+1)$ is true.

(iv) Then conclude by the Principle of Mathematical Induction (POMI) that $P(n)$ holds

Instructor's Comments: Emphasize the for some part in the IH step. Note also that the induction proof needn't start at 1 (it could start at 0 or -1 etc.)

Example: Prove that

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

for all $n \in \mathbb{N}$.

Proof: Let $P(n)$ be the statement that

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

holds. We prove $P(n)$ is true for all natural numbers n by the Principle of Mathematical Induction.

(i) Base case: When $n = 1$, $P(1)$ is the statement that

$$\sum_{i=1}^{1} i^2 = \frac{(1)((1)+1)(2(1)+1)}{6}.$$

This holds since

$$\frac{(1)((1)+1)(2(1)+1)}{6} = \frac{1(2)(3)}{6} = 1 = \sum_{i=1}^{1} i^2.$$

(ii) Inductive Hypothesis. Assume that $P(k)$ is true for some $k \in \mathbb{N}$. This means that

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}.$$

(iii) Inductive Step. We now need to show that

$$\sum_{i=1}^{k+1} i^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}.$$

To do this, we will start with the left hand side, reduce to the assumption made in the inductive hypothesis and then conclude the right hand side.

$$\begin{aligned}
\text{LHS} &= \sum_{i=1}^{k+1} i^2 \\
&= \sum_{i=1}^{k} i^2 + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 && \text{Inductive Hypothesis} \\
&= (k+1)\left(\frac{k(2k+1)}{6} + k + 1\right) \\
&= (k+1)\left(\frac{2k^2+k}{6} + \frac{6k+6}{6}\right) \\
&= (k+1)\left(\frac{2k^2+7k+6}{6}\right) \\
&= \frac{(k+1)(k+2)(2k+3)}{6} \\
&= \text{RHS}
\end{aligned}$$

Hence,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

is true for all natural numbers n by the Principle of Mathematical Induction. ■

Instructor's Comments: It is important to note where you used the inductive hypothesis!

Note: Now, we can finally solve the Tower of Hanoi example for the 100 level tower:

$$\begin{aligned}
V_{tower} &= \sum_{i=1}^{100} V_i \\
&= \sum_{i=1}^{100} \pi i^2 (1) \\
&= \pi \sum_{i=1}^{100} i^2 \\
&= \pi \frac{(100)(101)(2(100)+1)}{6} \\
&= 338350\pi
\end{aligned}$$

Instructor's Comments: This could easily be 25-30 minutes of your lecture. The rest of the time is spent doing examples:

Handout or Document Camera or Class Exercise

Prove that

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

holds for all natural numbers n.

Solution:

(i) Base case:

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

(ii) Inductive Hypothesis. Assume that

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

holds for some $k \in \mathbb{N}$

(iii) Inductive step. For $k+1$,

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) && \text{Inductive Hypothesis} \\
&= (k+1)(\tfrac{k}{2}+1) \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

Therefore, the claim holds by the Principle of Mathematical Induction for all $n \in \mathbb{N}$. ■

Instructor's Comments: This is the 40 minute mark

Instructor's Comments: An example where we don't start at 1

Example: Prove that $n! > 2^n$ for all $n \in \mathbb{N}$ with $n \geq 4$.

Proof: We proceed by mathematical induction.

(i) Base case: When $n = 4$, notice that $4! = 24 > 16 = 2^4$ so the inequality holds in this case.

(ii) Inductive Hypothesis: Assume that $k! > 2^k$ for some $k \in \mathbb{N}$ with $k \geq 4$.

(iii) Inductive Step: Notice that

$$\begin{aligned}
(k+1)! &= (k+1)k! \\
&> (k+1)2^k && \text{Inductive Hypothesis} \\
&> (1+1)2^k && \text{Since } k \geq 4 > 1 \\
&= 2^{k+1}
\end{aligned}$$

Thus, the conclusion holds for all $k \in \mathbb{N}$ with $k \geq 4$ by the Principle of Mathematical Induction. ■

Handout or Document Camera or Class Exercise

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.

Instructor's Comments: No base cases!

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.

Instructor's Comments: However, the logic of the inductive step is incorrect for n = 1, because the statement that "the two sets overlap" is false (there are only n + 1 = 2 horses prior to either removal, and after removal the sets of one horse each do not overlap. This is the 50 minute mark

Lecture 14

Handout or Document Camera or Class Exercise

Instructor's Comments: In this lecture, you might want to consider giving a midterm survey of your teaching.

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

Solution:

(i) Base case

$$2n^3 + 3n^2 + n = 2 + 3 + 1 = 6$$

and $6 \mid 6$. Hence $P(1)$ is true.

(ii) Inductive Hypothesis. Assume $P(k)$ is true for some $k \in \mathbb{N}$, that is, $\exists \ell \in \mathbb{Z}$ such that $6\ell = 2k^3 + 3k^2 + k$.

(iii) Inductive Step: Prove that $P(k+1)$ is true.

$$\begin{aligned} 2(k+1)^3 + 3(k+1)^2 + (k+1) &= 2k^3 + 6k^2 + 6k + 2 + 3k^2 + 6k + 3 + k + 1 \\ &= (2k^3 + 3k^2 + k) + 6k^2 + 12k + 6 \\ &= 6\ell + 6(k^2 + 2k + 1) && \text{IH} \\ &= 6(\ell + (k+1)^2) \end{aligned}$$

Hence, $6 \mid 2(k+1)^3 + 3(k+1)^2 + (k+1)$. Thus $P(k+1)$ is true. Hence by the Principle of Mathematical Induction, we have that $P(n)$ is true for all $n \in \mathbb{N}$. ■

Instructor's Comments: This is the 10 minute mark

Handout or Document Camera or Class Exercise

Instructor's Comments: This illustrates the need for something "stronger" than induction.

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 $k + 1$,

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

Only true if $k \geq 2$!!!

Instructor's Comments: This is the 15 minute mark

Principle of Strong Induction (POSI)

Axiom: If sequence of statements $P(1)$, $P(2)$, ... satisfy

(i) $P(1) \wedge P(2) \wedge ... \wedge P(b)$ are true for some $b \in \mathbb{N}$

(ii) $P(1) \wedge P(2) \wedge ... \wedge P(k)$ are true implies that $P(k+1)$ is true for all $k \in \mathbb{N}$

then $P(n)$ is true for all $n \in \mathbb{N}$.

Note: This is equivalent in strength to the Principle of Mathematical Induction and to the Well Ordering Principle!

Question: 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 strong induction.

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

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

For $n = 2$, we have $x_2 = 68$ and

$$2(-3)^2 + 10 \cdot 5^{2-1} = 18 + 50 = 68.$$

Inductive Hypothesis: Assume that

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

is true for all $i \in \{1, 2, ..., k\}$ for some $k \in \mathbb{N}$ and $k \geq 2$.

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

$$\begin{aligned}
x_{k+1} &= 2x_k + 15x_{k-1} && \text{Valid since } k \geq 2 \\
&= 2(2(-3)^k + 10 \cdot 5^{k-1}) + 15(2(-3)^{k-1} + 10 \cdot 5^{k-2}) \\
&= 4(-3)^k + 20 \cdot 5^{k-1} + 30(-3)^{k-1} + 150 \cdot 5^{k-2} \\
&= -12(-3)^{k-1} + 100 \cdot 5^{k-2} + 30(-3)^{k-1} + 150 \cdot 5^{k-2} \\
&= 18(-3)^{k-1} + 250 \cdot 5^{k-2} \\
&= 2 \cdot (-3)^2(-3)^{k-1} + 10 \cdot 5^2 \cdot 5^{k-2} \\
&= 2(-3)^{k+1} + 10 \cdot 5^k
\end{aligned}$$

Hence, $x_{k+1} = 2(-3)^{k+1} + 10 \cdot 5^k$. Thus, by the Principle of Strong Induction, we have that $x_n = 2(-3)^n + 10 \cdot 5^{n-1}$ for all $n \geq 1$. ■

Instructor's Comments: This is the 40 minute mark

Handout or Document Camera or Class Exercise

Instructor's Comments: I would make them do half of this example - say the base cases and the inductive hypothesis

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 $n \in \mathbb{N}$.

Proof: Let $P(n)$ be the given statement. We prove $P(n)$ by strong induction.

(i) Base cases: $P(1)$ is true since $x_1 = 3 < 4$ and $P(2)$ is true since $x_2 = 5 < 16 = 4^2$.

(ii) Inductive Hypothesis: Assume that $P(i)$ is true for all $i \in \{1, 2, ..., k\}$ for some $k \in \mathbb{N}$ with $k \geq 2$.

(iii) Inductive Step. For $k \geq 2$, we have

$$\begin{aligned} x_{k+1} &= 3x_k + 2x_{k-1} && \text{Valid since } k+1 \geq 3 \\ &< 3 \cdot 4^k + 2 \cdot 4^{k-1} \\ &< 4^{k-1}(3 \cdot 4 + 2) \\ &= 4^{k-1}(14) \\ &< 4^{k-1}(16) \\ &= 4^{k+1} \end{aligned}$$

Hence $P(k+1)$ is true and thus $P(n)$ is true for all $n \in \mathbb{N}$ by the Principle of Strong Induction.

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.

Note: For a cool link between this sequence and music, check out Tool - Lateralus on Youtube!

Instructor's Comments: This is the 50 minute mark

Lecture 15

Instructor's Comments: If you did the surveys, you could go over them at the beginning

Handout or Document Camera or Class Exercise

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 $\sum_{r=1}^{n} f_r^2 = f_n f_{n+1}$ for all $n \in \mathbb{N}$.

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

Solution: We prove only the first one. The second can be found on the Math 135 resources page

`http://www.cemc.uwaterloo.ca/~cbruni/Math135Resources.php`

(i) Base case: $n = 1$

$$\begin{aligned} \text{LHS} &= \sum_{r=1}^{n} f_r^2 \\ &= \sum_{r=1}^{1} f_r^2 \\ &= f_1^2 \\ &= 1^2 \\ &= 1 \end{aligned}$$

and

$$\text{RHS} = f_n f_{n+1} = f_1 f_2 = (1)(1) = 1 = \text{LHS}$$

(ii) Inductive Hypothesis. Assume that

$$\sum_{r=1}^{k} f_r^2 = f_k f_{k+1}$$

holds for some $k \in \mathbb{N}$.

(iii) Inductive Step. We want to show that

$$\sum_{r=1}^{k+1} f_r^2 = f_{k+1} f_{k+2}.$$

We begin with the left and proceed towards the right

$$\begin{aligned}
\text{LHS} &= \sum_{r=1}^{k+1} f_r^2 \\
&= \sum_{r=1}^{k} f_r^2 + f_{k+1}^2 \\
&= f_k f_{k+1} + f_{k+1}^2 && \text{Induction Hypothesis} \\
&= f_{k+1}(f_k + f_{k+1}) \\
&= f_{k+1} f_{k+2} && \text{By definition of Fibonacci Sequence} \\
&= \text{RHS}
\end{aligned}$$

Hence $\sum_{r=1}^{n} f_r^2 = f_n f_{n+1}$ for all $n \in \mathbb{N}$ by the Principle of Mathematical Induction. ■

Instructor's Comments: This easily is the 20-30 minute mark. Students might struggle with the notation.

Definition: Closed form: "Easy to put into a calculator" (This is not a formal definition!)

Example: Find a closed form expression for

$$P_n = \prod_{r=2}^{n} \left(1 - \frac{1}{r^2}\right)$$

where $n \geq 2$ and prove it is correct by induction.

Proof: We begin with some guessing and napkin (discovery) work.

$$P_2 = \prod_{r=2}^{2} \left(1 - \frac{1}{r^2}\right) = \left(1 - \frac{1}{2^2}\right) = 1 - \tfrac{1}{4} = \tfrac{3}{4}$$

$$P_3 = \prod_{r=2}^{3} \left(1 - \frac{1}{r^2}\right) = \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right) = (1 - \tfrac{1}{4})(1 - \tfrac{1}{9}) = \tfrac{3}{4} \cdot \tfrac{8}{9} = \tfrac{2}{3} = \tfrac{4}{6}$$

$$P_4 = \prod_{r=2}^{4} \left(1 - \frac{1}{r^2}\right) = \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{4^2}\right) = (1 - \tfrac{1}{4})(1 - \tfrac{1}{9})(1 - \tfrac{1}{16}) = \tfrac{3}{4} \cdot \tfrac{8}{9} \cdot \tfrac{15}{16} = \tfrac{5}{8}$$

Claim: $P_5 = \frac{6}{10}$ and in general $P_n = \frac{n+1}{2n}$ for all $n \geq 2$. We prove this by induction.

(i) Base case: $n = 2$

$$P_2 = \prod_{r=2}^{2} \left(1 - \frac{1}{r^2}\right) = \left(1 - \frac{1}{2^2}\right) = 1 - \tfrac{1}{4} = \tfrac{3}{4} = \tfrac{n+1}{2n}$$

(ii) Inductive Hypothesis. Assume that $P(k)$ is true for some $k \geq 2$ and $k \in \mathbb{N}$, that is, assume

$$\prod_{r=2}^{k} \left(1 - \frac{1}{r^2}\right) = \frac{k+1}{2k}$$

(iii) Inductive Step. We want to show that

$$\prod_{r=2}^{k+1} \left(1 - \frac{1}{r^2}\right) = \frac{(k+1)+1}{2(k+1)} = \frac{k+2}{2k+2}$$

We proceed starting from the left.

$$\begin{aligned}
\text{LHS} &= \prod_{r=2}^{k+1}\left(1-\frac{1}{r^2}\right) \\
&= \prod_{r=2}^{k}\left(1-\frac{1}{r^2}\right)\cdot\left(1-\frac{1}{(k+1)^2}\right) \\
&= \frac{k+1}{2k}\cdot\frac{(k+1)^2-1}{(k+1)^2} && \text{Inductive Hypothesis} \\
&= \frac{k+1}{2k}\cdot\frac{k^2+2k}{(k+1)^2} \\
&= \frac{k+1}{2k}\cdot\frac{k(k+2)}{(k+1)^2} \\
&= \frac{k+2}{2(k+1)} \\
&= \text{RHS}
\end{aligned}$$

Therefore, by the Principle of Mathematical Induction, we have that

$$P_n = \tfrac{n+1}{2n}$$

for all $n \geq 2$. ■

Instructor's Comments: This is the 50 minute mark.

Lecture 16

Handout or Document Camera or Class Exercise

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 $P(k+1)$.

Solution: Prove $P(1)$. Assume $P(k)$. Prove $P(k+1)$.

Instructor's Comments: This is the 5 minute mark.

Instructor's Comments: This is the last induction example - something slightly different.

Prove that an $m \times n$ chocolate bar consisting of unit squares can be broken into unit squares using

$$mn - 1$$

breaks.

Instructor's Comments: Mention below that the base case should be formally proven using induction but that we want. It will help to draw pictures as well. This is the first time that an induction question has two variables.

Proof: Let $m \in \mathbb{N}$ be fixed. We proceed by induction on n.

Base Case: When $n = 1$, we have an $m \times 1$ chocolate bar. This requires $m - 1$ breaks to get m unit squares (can prove formally by induction).

Inductive hypothesis: Assume that an $m \times k$ chocolate bar can be broken into unit squares using $mk - 1$ breaks for some $k \in \mathbb{N}$.

Inductive step: For an $m \times (k + 1)$ sized chocolate bar, we see that by breaking off the top row, gives a $m \times 1$ sized chocolate bar and a $m \times k$ sized chocolate bar. The first we know can be broken into unit squares using $m - 1$ breaks (this was the base case) and the latter can be broken into unit squares using $mk - 1$ breaks via the induction hypothesis. Hence, the total is

$$1 + m - 1 + mk - 1 = m(k + 1) - 1$$

as required. Hence, the claim is true for all $n \in \mathbb{N}$ by the Principle of Mathematical Induction.

Instructor's Comments: Again it helps to draw a picture above. We finish induction with the Fundamental Theorem of Arithmetic. Technically we can't prove it now but I will prove it up to Euclid's Lemma. This basically marks the midterm exam line in Fall2015 and Winter 2016.

Instructor's Comments: What you might want to do is do the following proof more informally and then return to it at the end of the term after more mathematical maturity has been developed and then redo this proof.

Theorem: (Euclid's Lemma [PAD - Primes and Divisibility]) Suppose $a, b \in \mathbb{Z}$ and p is a prime number. Show that if $p \mid ab$ then $p \mid a$ or $p \mid b$.

Corollary: (Generalized Euclid's Lemma) Suppose $a_1, a_2, ..., a_n \in \mathbb{Z}$ and p is a prime number. Show that if $p \mid a_1 a_2 ... a_n$ then $p \mid a_i$ for some integer $1 \leq i \leq n$.

Note: The proof of this lemma will be delayed until after we do some techniques through greatest common divisors. For now we will take this for granted and prove our first major theorem of the course. The generalization follows immediately.

Theorem: (Fundamental Theorem of Arithmetic) (UFT)

Every integer $n > 1$ can be factored uniquely as a product of prime numbers, up to reordering.

Note: Prime numbers are just the product of a single number.

Proof: Existence.

Assume towards a contradiction that not every number can be factored into prime numbers. Let n be the smallest such number (which exists by WOP). Then either n is prime, a contradiction, or $n = ab$ with $1 < a, b < n$. However, since $a, b < n$, the numbers a and b can be written as a product of primes (since n was minimal). Thus $n = ab$ is a product of primes, contradicting the definition of n.

Uniqueness

Assume towards a contradiction that there exists a natural number $n > 1$ such that

$$n = p_1 p_2 ... p_k = q_1 q_2 ... q_m$$

where each p_i and q_j are primes (not necessarily distinct) and further assume that this n is minimal (WOP). By definition, $p_1 \mid n = q_1 q_2 ... q_m$. Hence, by the generalized Euclid's Lemma, we see that $p_1 \mid q_j$ for some $1 \leq j \leq m$. Hence, since p_1 and q_j are prime numbers, we have that $p_1 = q_j$. Without loss of generality, we may reorder the primes q_j so that q_j is the first prime, that is, $p_1 = q_1$. Canceling out these primes gives

$$N_0 := p_2 ... p_k = q_2 ... q_m$$

Now $N_0 < n$ and so, the above representations must be equal up to reordering by the minimality of n. Hence, $k = m$ and we may reorder so that

$$p_\ell = q_\ell \qquad \text{for all } 2 \leq \ell \leq k$$

Multiplying N_0 by p_1 shows that the two representations of the factorizations of n are the same up to reordering. This contradicts the existence of n hence all numbers can be written uniquely as a product of primes up to reordering of primes.

Instructor's Comments: This is a difficult proof. I would advise taking some time and really going through it. If you're lucky this will take you to just the 50 minute mark.

Lecture 17

Theorem: (Euclid's Theorem) (INF P) There exists infinitely many primes.

Proof: Assume towards a contradiction that there exists finitely many primes, say $p_1, p_2, ..., p_n$. Consider the number

$$N = 1 + \prod_{i=1}^{n} p_i$$

By the Fundamental Theorem of Arithmetic (UFT), N can be written as a product of primes. In particular, there exists a prime $p \mid N$ by the Generalized Euclid's Lemma. Since we have only finitely many primes, $p = p_1$ for some $1 \leq i \leq n$. Since $p \mid N$ and $p \left| \prod_{i=1}^{n} p_i \right.$, we conclude by Divisibility of Integer Combinations that

$$p \left| \left(N - \prod_{i=1}^{n} p_i \right) \right. = 1$$

This is a contradiction since no prime divides 1 (you could use Bounds by Divisibility since primes are bigger than 1). Hence, there must be infinitely many primes. ■

To complete the gaps in the previous proofs, we need to talk about the two forms of Euclid's Lemma. To do this, we will need to talk about greatest common divisors and more importantly, Bézouts Lemma.

Instructor's Comments: This is the 7-10 minute mark

Greatest Common Divisors

Instructor's Comments: Arguably, this is the toughest portion of the course. These arguments for gcds are often tricky and counter intuitive and take a bit of practice before mastering.

As an exercise, let's list the divisors of 84:

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 7, \pm 12, \pm 14, \pm 21, \pm 28, \pm 42, \pm 81$$

Divisors of 120:

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 8, \pm 10, \pm 12, \pm 15, \pm 20, \pm 24, \pm 30, \pm 40, \pm 60, \pm 120$$

Hence the greatest common divisors of 84 and 120 is 12.

Definition: The *greatest common divisors* of integers a and b with $a \neq 0$ or $b \neq 0$ is an integer $d > 0$ such that

(i) $d \mid a$ and $d \mid b$

(ii) If $c \mid a$ and $c \mid b$, then $c \leq d$

We write $d = \gcd(a, b)$.

Note:

(i) $\gcd(a, a) = |a| = \gcd(a, 0)$

(ii) Define $\gcd(0, 0) = 0$. Note that $\gcd(a, b) = 0 \Leftrightarrow a = b = 0$

(iii) **Exercise:** $\gcd(a, b) = \gcd(b, a)$

Instructor's Comments: This is the 20 minute mark

Handout or Document Camera or Class Exercise

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

Proof: . Let $d = \gcd(3a+b, a)$ and $e = \gcd(a, b)$. Then by definition, $d \mid (3a+b)$ and $d \mid a$. By Divisibility of Integer Combinations,

$$d \mid (3a+b) - 3a = b$$

Since e is the maximal divisor of a and b, we have that $d \leq e$.

Now, since $e \mid a$ and $e \mid b$, Divisibility of Integer Combinations gives us that $e \mid (3a+b)$. Since d is maximal, $e \leq d$. Hence $d = e$. ■

Instructor's Comments: This is the 30 minute mark

Claim: $\gcd(a, b)$ exists.

Proof: Suppose that $a \neq 0$ or $b \neq 0$. Clearly $1 \mid a$ and $1 \mid b$ so a divisor exists.

To show there is a greatest common divisor, it suffices to show that there is an upper bound on common divisors of a and b. If d is a positive integer such that $d \mid a$ and $d \mid b$, then Bounds by Divisibility states that $d \leq |a|$ and $d \leq |b|$. Hence,

$$1 \leq d \leq \min\{|a|, |b|\}$$

Since the range on divisors is bounded, there must be a maximum. ■

Claim: $\gcd(a, b)$ is unique.

Proof: Suppose d and e are both the greatest common divisors of a and b. Then $d \mid a$ and $d \mid b$. Thus, since e is maximal, $d \leq e$. Similarly, $e \leq d$. Hence $d = e$.

Instructor's Comments: This is the 40 minute mark

Suppose we wanted to find a divisors of two numbers a and b. Can we do so? How far do we have to look? Here is a theorem explaining this.

Proposition: (Finding a Prime Factor) (FPF) Let $a, b \in \mathbb{N}$. If $n = ab$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof: Suppose $n = ab$ and $a > \sqrt{n}$. Then

$$\begin{aligned} ab &> b\sqrt{n} \\ n &> b\sqrt{n} \\ \sqrt{n} &> b \end{aligned}$$

Hence $b \leq \sqrt{n}$. ■

Instructor's Comments: This is the 45 minute mark. From this point on in the course, the theorem cheat sheets on the Math 135 Resources page will be quite useful for students. There will be many named theorems that students will be expected to know.. Don't rush the next example. Maybe do it in this lecture and review it a bit in the next lecture. GCDWR works very well if the two parameters in the greatest common divisor depend on each other in some way.

Proposition: GCD With Remainder (GCDWR) If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

Example: $\gcd(72, 40) = 8$. Now, $72 = 40(2) - 8$ and so GCD With Remainder says that

$$\gcd(72, 40) = \gcd(40, -8) = 8$$

Note that this looks similar to the division algorithm, but the 'remainder' here can be negative. You can apply this multiple times to help reduce the gcd computation a lot (this we will see later).

Instructor's Comments: Delay the proof until next class. Talk about the previous example more - maybe even It's included here only if my timings above are incorrect.

Proof: (of GCDWR) If $a = b = 0$, then $r = a - bq = 0$. Hence $\gcd(a, b) = 0 = \gcd(b, r)$. Now assume that $a \neq 0$ or $b \neq 0$. Let $d = \gcd(a, b)$ and $e = \gcd(b, r)$. Since $a = bq + r$ and $d \mid a$ and $d \mid b$, by Divisibility of Integer Combinations, $d \mid (a - bq) = r$. Thus, since e is the maximal common divisor of b and r, we see that $d \leq e$.

Now, $e \mid b$ and $e \mid r$ so by Divisibility of Integer Combinations, $e \mid (bq + r) = a$. Since d is the largest divisor of a and b, we see that $e \leq d$.

Hence $d = e$. ■

Lecture 18

Proposition: GCD With Remainder (GCDWR) If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$

Proof: (of GCDWR) If $a = b = 0$, then $r = a - bq = 0$. Hence $\gcd(a, b) = 0 = \gcd(b, r)$. Now assume that $a \neq 0$ or $b \neq 0$. Let $d = \gcd(a, b)$ and $e = \gcd(b, r)$. Since $a = bq + r$ and $d \mid a$ and $d \mid b$, by Divisibility of Integer Combinations, $d \mid (a - bq) = r$. Thus, since e is the maximal common divisor of b and r, we see that $d \leq e$.

Now, $e \mid b$ and $e \mid r$ so by Divisibility of Integer Combinations, $e \mid (bq + r) = a$. Since d is the largest divisor of a and b, we see that $e \leq d$.

Hence $d = e$. ■

Instructor's Comments: This is the 7-10 minute mark

Handout or Document Camera or Class Exercise

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

Solution: $3s + t = (3)s + t$. Thus, GCD With Remainders states that $\gcd(3s+t, s) = \gcd(s, t)$ by setting $a = 3s + t$, $b = s$, $q = 3$ and $r = t$. ■

Instructor's Comments: This is the 15 minute mark

Euclidean Algorithm How can we compute the greatest common divisor of two numbers quickly? This is where we can combine GCD With Remainders and the Division Algorithm in a clever way to come up with an efficient algorithm discovered over 2000 years ago that is still used today.

Example: Compute $\gcd(1239, 735)$.

Solution:

$$\begin{aligned} 1239 &= 735(1) + 504 && \text{Eqn 1} \\ 725 &= 504(1) + 231 && \text{Eqn 2} \\ 504 &= 231(2) + 42 && \text{Eqn 3} \\ 231 &= 42(5) + 21 && \text{Eqn 4} \\ 42 &= 21(1) + 0 \end{aligned}$$

Thus, by GCDWR, we have

$$\begin{aligned} \gcd(1239, 735) &= \gcd(735, 504) \\ &= \gcd(504, 231) \\ &= \gcd(231, 42) \\ &= \gcd(42, 21) \\ &= \gcd(21, 0) \\ &= 21 \end{aligned}$$

Note: This process stops since remainders form a sequence of non-negative decreasing integers. In this process, the greatest common divisor is the last nonzero remainder.

Instructor's Comments: This is the 25 minute mark

Question: Food for thought: What is the runtime of the Euclidean Algorithm?

Back Substitution Remember our goal for GCDs is to prove Euclid's Lemma. It turns out that this question is deeply connected to the following question:

Question: Do there exist integers x and y such that $ax + by = \gcd(a, b)$?

It turns out that the answer to this question is yes! This result is known as Bézout's Lemma (or EEA in this course). We first show this is true in an example by using the method of Back Substitution and then later using the Extended Euclidean Algorithm. Using the $\gcd(1239, 735) = 21$ example from before, we start with the last line and work our way backwards to see:

$$\begin{aligned} 21 &= 231(1) + 42(-5) && \text{By Eqn 4} \\ &= 231(1) + (504(1) + 231(-2))(-5) && \text{By Eqn 3} \\ &= 231(11) + 504(-5) \\ &= (735(1) + 504(-1))(11) + 504(-5) && \text{By Eqn 2} \\ &= 735(11) + 504(-16) \\ &= 735(11) + (1239 + 735(-1))(-16) && \text{By Eqn 1} \\ &= 735(27) + 1239(-16) \end{aligned}$$

Instructor's Comments: This is the 35 minute mark

Handout or Document Camera or Class Exercise

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

Instructor's Comments: If a student finishes quickly, challenge them to find two such linear combinations.

Solution:

$$\begin{aligned} 120 &= 84(1) + 36 \\ 84 &= 36(2) + 12 \\ 36 &= 12(3) + 0 \end{aligned}$$

Thus, by the Euclidean Algorithm (or by GCDWR), we have that $\gcd(120, 84) = 12$. Next,

$$\begin{aligned} 12 &= 84 + 36(-2) \\ &= 84 + (120 + 84(-1))(-2) \\ &= 84(3) + 120(-2) \end{aligned}$$

Note: Food for thought: Note also that $84(3 + 120) + 120(-2 - 84)$ will also work and so on.

Instructor's Comments: This is the 45 minute mark

Theorem: (Bézout's Lemma (Extended Euclidean Algorithm - EEA)) Let $a, b \in \mathbb{Z}$. Then there exist integers x, y such that $ax + by = \gcd(a, b)$

Proof: We've seen the outline of the proof via an example. Just make the argument abstract. The proof is left as a reading exercise. ■

Theorem: GCD Characterization Theorem (GCDCT) If $d > 0$, $d \mid a$, $d \mid b$ and there exist integers x and y such that $ax + by = d$, then $d = \gcd(a, b)$.

Proof: Let $e = \gcd(a, b)$. Since $d \mid a$ and $d \mid b$, by definition and the maximality of e we have that $d \leq e$. Again by definition, $e \mid a$ and $e \mid b$ so by Divisibility of Integer Combinations, $e \mid (ax + by)$ implying that $e \mid d$. Thus, by Bounds by Divisibility, $|e| \leq |d|$ and since $d, e > 0$, we have that $e \leq d$. Hence $d = e$. ■

Instructor's Comments: This is the 50 minute mark

Lecture 19

Instructor's Comments: Do these proofs if you missed them. Otherwise review the theorems with examples.

Theorem: (Bézout's Lemma (Extended Euclidean Algorithm - EEA)) Let $a, b \in \mathbb{Z}$. Then there exist integers x, y such that $ax + by = d$

Proof: We've seen the outline of the proof via an example. Just make the argument abstract. The proof is left as a reading exercise. ■

Theorem: GCD Characterization Theorem (GCDCT) If $d > 0$, $d \mid a$, $d \mid b$ and there exist integers x and y such that $ax + by = d$, then $d = \gcd(a, b)$.

Proof: Let $e = \gcd(a, b)$. Since $d \mid a$ and $d \mid b$, by maximality we have that $d \leq e$. Now $e \mid a$ and $e \mid b$ so by Divisibility of Integer Combinations, $e \mid (ax + by) = d$. Thus, by Bounds by Divisibility, $|e| \leq |d|$ and since $d, e > 0$, we have that $e \leq d$. Hence $d = e$. ■

Example: $6 > 0$, $6 \mid 30$, $6 \mid 42$ and $30(3) + 42(-2) = 6$ and hence by the GCD Characterization Theorem, we have that $\gcd(30, 42) = 6$.

Example: Prove if $a, b, x, y \in \mathbb{Z}$, are such that $\gcd(a, b) \neq 0$ and $ax + by = \gcd(a, b)$, then $\gcd(x, y) = 1$.

Proof: Since $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, we divide by $\gcd(a, b) \neq 0$ to see that

$$\frac{a}{\gcd(a, b)}x + \frac{b}{\gcd(a, b)}y = 1$$

Since $1 \mid x$ and $1 \mid y$ and $1 > 0$, GCD Characterization Theorem implies that $\gcd(x, y) = 1$. ■

Instructor's Comments: This is the 10 minute mark.

Now, we've reached the point where we can prove Euclid's Lemma.

Theorem: (Euclid's Lemma - [Primes and Divisibility PAD]). If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: Suppose p is prime, $p \mid ab$ and $p \nmid a$ (possible by elimination). Since $p \nmid a$, $\gcd(p, a) = 1$. By Bézout's Lemma, there exist $x, y \in \mathbb{Z}$ such that

$$px + ay = 1$$
$$pbx + aby = b$$

Now, since $p \mid p$ and $p \mid ab$, by Divisibility of Integer Combinations, $p \mid p(bx) + ab(y)$ and hence $p \mid b$.

Instructor's Comments: This is the 20 minute mark

Handout or Document Camera or Class Exercise

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 $ax^2 + by^2 = c$.

Solution:

(i) $n + 1 = n(1) + 1$ and so by the GCD Characterization Theorem, $\gcd(n+1, n) = \gcd(n, 1) = 1$. Hence this is true.

(ii) $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$. Thus, by Divisibility of Integer Combinations, $\gcd(a, b) \mid (ax^2 + by^2)$ which implies that $\gcd(a, b) \mid c$. Hence this is true.

(iii) This is false. Suppose that $a = 3$, $b = 0$ and $c = 6$. Then $\gcd(a, b) = 3 \mid 6 = c$ however, $3x^2 + 0y^2 = 6$ implies that $x^2 = 2$, a contradiction.

Instructor's Comments: This is the 30-35 minute mark. At the end of this lecture, I think it would be wise to talk about the midterm a bit. It is coming up so I've left a bit of extra time to review for the midterm.

Lecture 20

Handout or Document Camera or Class Exercise

Instructor's Comments: This is where things might start to differ. The idea at this point is to make the Monday lecture the Extended Euclidean Algorithm because this is a computational topic and it would help ease the lecture before the midterm. Thus, this lecture and lecture 21 can be swapped without harm. I'm going to give the gcd theorem lecture here and delay the EEA lecture until Lecture 21.

Instructor's Comments: This may or may not be a Friday lecture. Friday lectures I reserve time to do a clicker question. Modify accordingly.

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

Solution: The first is false. Consider $a = b = -1$. The second is true (use the contrapositive). The third is true by definition (mention the $a = b = 0$ case). The fourth is also true by definition. The fifth is true again by definition.

In this lecture, we'll go over some key gcd theorems that you will need to prove some problems on your assignment.

Instructor's Comments: IMPORTANT TIP: If the gcd condition appears in the hypothesis, then Bézout's Lemma (EEA) might be useful. If the gcd condition appears in the conclusion, then GCDCT might be useful. It might be good to rewrite GCDCT on the board: if d is a positive integer and a common divisor of a and b and gcd(a,b) is an integer linear combination of a,b. Then gcd(a,b) = d.

Handout or Document Camera or Class Exercise

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.

Proof: By Bézout's Lemma, there exists $x, y \in \mathbb{Z}$ such that $ab(x) + c(y) = 1$. Since $1 \mid a$ and $1 \mid c$ and $a(bx) + c(y) = 1$, by the GCD Characterization Theorem, $\gcd(a, c) = 1$. Similarly, $\gcd(b, c) = 1$. ■

Proof: If $\gcd(a, c) = \gcd(b, c) = 1$, then $\gcd(ab, c) = 1$. Since $\gcd(a, c) = 1$, Bézout's Lemma, there exists integers x and y such that $ax+cy = 1$. Similarly, there exists integers k and m such that $bk + cm = 1$. Multiplying gives

$$\begin{aligned} 1 &= (ax + cy)(bx + cm) \\ &= abx^2 + acxm + bcyx + c^2ym \\ &= abx^2 + c(axm + byx + xym) \end{aligned}$$

Since $1 \mid ab$, $1 \mid c$ and $1 > 0$, by GCD Characterization theorem, $\gcd(ab, c) = 1$. ■

Instructor's Comments: This is the 10-15 minute mark

Note: IMPORTANT TIP: If the gcd condition appears in the hypothesis, then EEA or Bézout's theorem is useful. If the gcd condition appears in the conclusion, then GCDCT is useful.

Proposition: (GCD of One) (GCDOO). Let $a, b \in \mathbb{Z}$. Then $\gcd(a, b) = 1$ if and only if there exists integers x and y such that $ax + by = 1$.

Proof: Suppose $\gcd(a, b) = 1$. Then by Bézout's Lemma, there exists integers x and y such that $ax + by = 1$.

Now, suppose that there exist integers x and y such that $ax + by = 1$. Then since $1 \mid a$ and $1 \mid b$, then by the GCD Characterization Theorem, $\gcd(a, b) = 1$. ■

Instructor's Comments: This is the 25 minute mark

Proposition: Division by the GCD (DBGCD). Let $a, b \in \mathbb{Z}$. If $\gcd(a, b) = d$ and $d \neq 0$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof: Suppose that $\gcd(a, b) = d \neq 0$. Then by Bézout's Lemma, there exist integers x and y such that $ax + by = d$. Dividing by the nonzero d gives $\frac{a}{d}x + \frac{b}{d}y = 1$. Thus, by GCDOO, we see that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. ■

Example: Let $a = 91$ and $b = 70$. Then $\gcd(a, b) = 7$ and by DBGCD, we have that

$$1 = \gcd(\tfrac{a}{d}, \tfrac{b}{d}) = \gcd(\tfrac{91}{7}, \tfrac{70}{7}) = \gcd(13, 10).$$

Instructor's Comments: This is the 35-37 minute mark

Definition: We say that two integers a and b are coprime if $\gcd(a, b) = 1$.

Proposition: Coprimeness and Divisibility (CAD). If $a, b, c \in \mathbb{Z}$ and $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$.

Proof: Suppose that $\gcd(a, c) = 1$ and $c \mid ab$. Since $\gcd(a, c) = 1$, by Bézout's Lemma, there exists integers x and y such that $ax + cy = 1$. Multiplying by b gives $abx + cby = b$. Since $c \mid ab$ and $c \mid c$, by Divisibility of Integer Combinations, we have that $c \mid (ab(x) + c(by))$ and hence $c \mid b$. ■

Example: Let $a = 14$, $b = 30$ and $c = 15$. Then $c \mid ab$ since $15 \mid (14)(30) = 420$ and $\gcd(a, c) = \gcd(14, 15) = 1$. Thus, by CAD, $c \mid b$ or $15 \mid 30$.

Instructor's Comments: This is the 50 minute mark. Remind students of the theorem cheat sheets on the website.

Lecture 21

Instructor's Comments: This should be the lecture you give on the day of the midterm. It is a very light computational lecture.

Definition: For $x \in \mathbb{R}$, define the floor function $\lfloor x \rfloor$ to be the greatest integers less than or equal to x.

Example:

(i) $\lfloor 2.5 \rfloor = 2 = \lfloor 2 \rfloor$

(ii) $\lfloor \pi \rfloor = 3$

(iii) $\lfloor 0 \rfloor = 0$

(iv) $\lfloor -2.5 \rfloor = -3$

Example: Find $\gcd(56, 35)$

$$
\begin{aligned}
56(1) + 35(0) &= 56 && \text{Eqn } [1] \\
56(0) + 35(1) &= 35 && \text{Eqn } [2] \\
56(1) + 35(-1) &= 21 && q_1 = \lfloor \tfrac{56}{35} \rfloor = 1 \text{ Eqn } [3] = [1] - q_1[2] \\
56(-1) + 35(2) &= 14 && q_2 = \lfloor \tfrac{35}{21} \rfloor = 1 \text{ Eqn } [4] = [2] - q_2[3] \\
56(2) + 35(-3) &= 7 && q_3 = \lfloor \tfrac{21}{14} \rfloor = 1 \text{ Eqn } [5] = [3] - q_3[4] \\
56(-5) + 35(8) &= 0 && q_4 = \lfloor \tfrac{14}{7} \rfloor = 2 \text{ Eqn } [6] = [4] - q_4[5]
\end{aligned}
$$

Therefore $\gcd(56, 35) = 7 = 56(2) + 35(-3)$. This process gives rise to the Extended Euclidean Algorithm.

Example: Find $x, y \in \mathbb{Z}$ such that $506x + 391y = \gcd(506, 391)$.

x	y	r	q
1	0	506	0
0	1	391	0
1	-1	115	$\lfloor \frac{506}{391} \rfloor = 1$
-3	4	46	$\lfloor \frac{391}{115} \rfloor = 3$
7	-9	23	$\lfloor \frac{115}{46} \rfloor = 2$
-17	22	0	$\lfloor \frac{46}{23} \rfloor = 2$

Therefore, $506(7) + 391(-9) = 23 = \gcd(506, 391)$. ■

Note: This process is known as the Extended Euclidean Algorithm.

Handout or Document Camera or Class Exercise

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

Solution:

x	y	r	q
1	0	408	0
0	1	170	0
1	-2	68	$\lfloor \frac{408}{170} \rfloor = 2$
-2	5	34	$\lfloor \frac{170}{68} \rfloor = 2$
5	-12	0	$\lfloor \frac{68}{34} \rfloor = 2$

Therefore, $408(-2) + 170(5) = 34 = \gcd(408, 170)$. ■

Note:

(i) Bézout's Lemma is the Extended Euclidean Algorithm in the textbook.

(ii) With $\gcd(a, b)$, what if

1. $b > a$? Then swap a and b. This works since $\gcd(a, b) = \gcd(b, a)$.
2. $a < 0$ or $b < 0$? Solution is to make all the terms positive. This works since

$$\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b).$$

(iii) In practice, one can accomplish these goals by changing the headings then accounting for this in the final steps.

Handout or Document Camera or Class Exercise

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

Solution:

x	$-y$	r	q
0	1	2145	0
1	0	399	0
-5	1	150	$\lfloor \frac{2145}{399} \rfloor = 5$
11	-2	99	$\lfloor \frac{399}{150} \rfloor = 2$
-16	3	51	$\lfloor \frac{150}{99} \rfloor = 1$
27	-5	48	$\lfloor \frac{99}{51} \rfloor = 1$
-43	8	3	$\lfloor \frac{51}{48} \rfloor = 1$
27-(16)(-43)	-5-16(8)	0	$\lfloor \frac{48}{3} \rfloor = 1$

Therefore, $x = -43$, $-y = 8$ and so $y = -8$, $\gcd(399, -2145) = 3$. Hence

$$399(-43) - 2145(-8) = 3 = \gcd(399, -2145)$$

Lecture 22

Instructor's Comments: One thing I noticed that I want to spend a bit of time going over at the beginning was how to write a factorization of a number n

Recall: Fundamental Theorem of Arithmetic. Suppose that $n > 1$ is an integer. Then n can be factored uniquely as a product of prime numbers up to reordering of prime numbers.

Note: For a natural number n we can write down this factorization in a number of ways:

(i) $n = \prod_{i=1}^{k} p_i$ where each p_i is prime. ($n > 1$ required)

(ii) $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ where each $\alpha_i \geq 1$ is an integer and each p_i is distinct. ($n > 1$ required)

(iii) $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ where each $\alpha_i \geq 0$ is an integer and each p_i is distinct. This is useful if you have two numbers and want to write them using the same primes p_i. They might not have the same prime factors, but allowing for the exponent to be 0 allows you to write them using the same prime factors. For example, $30 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0$ and $14 = 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^1$.

Instructor's Comments: This is the 5 minute mark.

Theorem: Divisors From Prime Factorization (DFPF). Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ where each $\alpha_i \geq 1$ is an integer. Then d is a positive divisor of n if and only if a prime factorization of d can be given by

$$d = \prod_{i=1}^{k} p_i^{\delta_i} \qquad \text{where } \delta_i \in \mathbb{Z}, 0 \leq \delta_i \leq \alpha_i \text{ for } 1 \leq i \leq k$$

Proof: Extra reading. ■

Example: Positive divisors of $63 = 3^2 \cdot 7$ are given by

$$3^0 \cdot 7^0, 3^0 \cdot 7^1, 3^1 \cdot 7^0, 3^1 \cdot 7^1, 3^2 \cdot 7^0, 3^2 \cdot 7^1$$

or

$$1, 7, 3, 21, 9, 63$$

Instructor's Comments: This is the 15 minute mark

Handout or Document Camera or Class Exercise

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

Solution: Notice that $2940 = 12(245)$ (say by long division). Then, to find the number of divisors of 2940 that are multiples of 12, you just need to take the divisors of 245 (and then multiply them all by 12). Since $245 = 5 \cdot 7^2$, the total number of divisors is $(1+1)(2+1) = 6$.

Instructor's Comments: Explain to students this is like taking 0 or 1 five and then 0, 1, or 2 sevens.

Hence the multiples are:

$$12, 12 \cdot 5, 12 \cdot 7, 12 \cdot 5 \cdot 7, 12 \cdot 7^2, 12 \cdot 5 \cdot 7^2$$

Instructor's Comments: This is the 25 minute mark

Example: Prove that $a^2 \mid b^2$ if and only if $a \mid b$.

Proof: Assume that $a \mid b$. Then there exists a $k \in \mathbb{Z}$ such that $ak = b$. Now $a^2k^2 = b^2$ and hence $a^2 \mid b^2$ by definition.

Now, assume that $a^2 \mid b^2$. For convenience, assume that $a, b > 0$. Now, write

$$a = \prod_{i=1}^{k} p_i^{\alpha_i} \qquad b = \prod_{i=1}^{k} p_i^{\beta_i}.$$

where $0 \leq \alpha_i$ and $0 \leq \beta_i$ are integers and the p_i are distinct primes. Since $a^2 \mid b^2$, we have that

$$\prod_{i=1}^{k} p_i^{2\alpha_i} \;\Bigg|\; \prod_{i=1}^{k} p_i^{2\beta_i}$$

Now, Divisors From Prime Factorization implies that $2\alpha_i \leq 2\beta_i$ and so $\alpha_i \leq \beta_i$ true for $1 \leq i \leq k$. Divisors From Prime Factorization again implies that

$$a = \prod_{i=1}^{k} p_i^{\alpha_i} \;\Bigg|\; \prod_{i=1}^{k} p_i^{\beta_i} = b$$

as required. ■

Instructor's Comments: One more theorem. This is the 35 minute mark

Example:

$$\begin{aligned} \gcd(2^5 \cdot 3^0 \cdot 5^4, 2^4 \cdot 3^1 \cdot 5^4) &= 2^{\min\{4,5\}} \cdot 3^{\min\{0,1\}} \cdot 5^{\min\{4,4\}} \\ &= 2^4 \cdot 5^4 \\ &= 10000 \end{aligned}$$

Instructor's Comments: Mention that factoring is very complicated.

Theorem: (GCD From Prime Factors (GCDPF)) If

$$a = \prod_{i=1}^{k} p_i^{\alpha_i} \qquad b = \prod_{i=1}^{k} p_i^{\beta_i}.$$

where $0 \leq \alpha_i$ and $0 \leq \beta_i$ are integers and the p_i are distinct primes, then

$$\gcd(a, b) = \prod_{i=1}^{k} p_i^{m_i}$$

where $m_i = \min\{\alpha_i, \beta_i\}$ for $1 \leq i \leq k$.

Proof: More extra reading. ■

Instructor's Comments: The next topic is completely optional on least common multiples. Do it if you have time

Let $\text{lcm}(a, b)$ represent the least common multiple of a and b.

Example:

(i) Write out a formal definition of $\text{lcm}(a, b)$.

(ii) Show that $\text{lcm}(a, b) = \prod_{i=1}^{k} p_i^{e_i}$ where $e_i = \max\{\alpha_i, \beta_i\}$.

(iii) Prove that $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.

Instructor's Comments: Lastly, I give tips for solving GCD problems. The analogy is going to Toronto: Taking the 401 (might be hard but is ideal). Walking (Slow but will get you there). Flying (Theoretically fastest but takes longer to set up) These are continued on the lecture if you run out of time.

When solving GCD problems, the following gives a rough order of how and when you should try a technique

(i) Bézout's Theorem (EEA) [Good when gcd is in hypothesis]

(ii) GCDWR [Good when terms in gcd depend on each other; good for computations]

(iii) GCDCT [Good when gcd is in conclusion]

(iv) Definition [Good when nothing else seems to work]

(v) GCDPF [Good when you're desperate]

Lecture 23

Instructor's Comments: If you ran out of time last lecture, you should give students the following tips.

When solving GCD problems, the following gives a rough order of how and when you should try a technique

(i) Bézout's Theorem (EEA) [Good when gcd is in hypothesis]

(ii) GCDWR [Good when terms in gcd depend on each other; good for computations]

(iii) GCDCT [Good when gcd is in conclusion]

(iv) Definition [Good when nothing else seems to work]

(v) GCDPF [Good when you're desperate]

Handout or Document Camera or Class Exercise

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) $143x + 253y = 154$

Instructor's Comments: The answers to these questions will be part of the lecture today.

Linear Diophantine Equations (LDE)

We want to solve $ax + by = c$ where $a, b, c \in \mathbb{Z}$ under the condition that $x, y \in \mathbb{Z}$

Instructor's Comments: Relate this to solving for the equation of a line over the real case and invite students to think critically about the difference in the integer case.

Example: Solve the LDE $143x + 253y = 11$.

Solution: We can solve this using the Extended Euclidean Algorithm!

x	y	r	q
0	1	253	
1	0	143	
-1	1	110	1
2	-1	33	1
-7	4	11	3
23	-13	0	3

Therefore, $143(-7) + 254(4) = 11$. Are there other solutions?

Instructor's Comments: This is the 10-15 minute mark depending on the introduction. Students should do the EEA on their own and you should do it simultaneously.

Questions to ask about LDE's

(i) Is there a solution?

(ii) What is it?

(iii) Are there more than one?

Example: Solve the LDE

$$143x + 253y = 155$$

Solution: Assume towards a contradiction that there exist x_0 and y_0 integers such that

$$143x_0 + 253y_0 = 155$$

By before, $11 \mid 143$ and $11 \mid 253$. Hence by Divisibility of Integer Combinations, $143x_0 + 253y_0$ is divisible by 11. HOWEVER,

$$11 \nmid 155 = 143x_0 + 253y_0$$

which is a contradiction. Hence the original LDE has no integer solutions. ■

Instructor's Comments: This is the 25 minute mark.

What about

$$143x + 253y = 154$$

as an LDE? Now, notice that $154 = 11 \cdot 14$. Hence, since

$$143(-7) + 253(4) = 11$$

multiplying by 14 gives

$$143(-7 \cdot 14) + 253(4 \cdot 14) = 11 \cdot 14$$
$$143(-98) + 253(56) = 154$$

Instructor's Comments: This is the 35 minute mark.

These insights lead to the following theorem

Theorem: (LDET1) Let $d = \gcd(a, b)$. The LDE

$$ax + by = c$$

has a solution if and only if $d \mid c$.

Proof: ($\Rightarrow$) Assume that $ax + by = c$ has an integer solution, say $x_0, y_0 \in \mathbb{Z}$. Since $d \mid a$ and $d \mid b$, by Divisibility of Integer Combinations, we have that $d \mid (ax_0 + by_0) = c$.

($\Leftarrow$) Assume that $d \mid c$. Then, there exists an integer k such that $dk = c$. By Bézout's Lemma, there exist integers u and v such that $au + bv = \gcd(a, b) = d$. Multiplying by k gives

$$a(uk) + b(vk) = dk = c$$

Therefore, a solution is given by $x = uk$ and $y = vk$. ■

Instructor's Comments: This is the 45 minute mark.

Example: Solve $20x + 35y = 5$ as an LDE.

Solution: Notice here that we can simplify the LDE by dividing by 5 first to give

$$4x + 7y = 1$$

An easy solution is given by $x = 2$ and $y = -1$.

Now, look at $x_2 = 2 + 7$ and $y_2 = -1 - 4$. Notice that

$$\begin{aligned} 4x_2 + 7y_2 &= 4(2 + 7) + 7(-1 - 4) \\ &= 4(2) + 4(7) + 7(-1) + 7(-4) \\ &= 4(2) + 7(-1) \\ &= 4x + 7y \\ &= 1 \end{aligned}$$

In fact, if I take $x_2 = 2 + 7(11)$ and $y_2 = -1 - 4(11)$. Notice that

$$\begin{aligned} 4x_2 + 7y_2 &= 4(2 + 7(11)) + 7(-1 - 4(11)) \\ &= 4(2) + 4(7)(11) + 7(-1) + 7(-4)(11) \\ &= 4(2) + 7(-1) \\ &= 4x + 7y \\ &= 1 \end{aligned}$$

and 11 above is very arbitrary. In fact, this gives us an insight into the complete characterization of solutions for an LDE.

Lecture 24

Handout or Document Camera or Class Exercise

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 $\gcd(ax, by) = 6$.

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

Theorem: (LDET2) Let $d = \gcd(a, b)$ where $a \neq 0$ and $b \neq 0$. If $(x, y) = (x_0, y_0)$ is a solution to the LDE

$$ax + by = c$$

then all solutions are given by

$$x = x_0 + \tfrac{b}{d}n \qquad y = y_0 - \tfrac{a}{d}n$$

for all $n \in \mathbb{Z}$. Alternatively, the solution set is given by

$$\{(x_0 + \tfrac{b}{d}n, y_0 - \tfrac{a}{d}n) : n \in \mathbb{Z}\}$$

Proof: Note that the above are actually solutions to the LDE. It suffices to show that these are all the solutions. Let (x, y) be a different solution to the LDE (other than (x_0, y_0)). Then,

$$\begin{aligned} ax + by &= c \\ ax_0 + by_0 &= c \end{aligned}$$

Subtracting gives

$$\begin{aligned} a(x - x_0) + b(y - y_0) &= 0 \\ a(x - x_0) &= -b(y - y_0) \\ \tfrac{a}{d}(x - x_0) &= \tfrac{-b}{d}(y - y_0) \end{aligned}$$

Now, since $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ (by DBGCD) and since

$$\tfrac{b}{d} \mid \tfrac{-b}{d}(y - y_0) = \tfrac{a}{d}(x - x_0)$$

we use Coprimeness and Divisibility (CAD) to see that $\frac{b}{d} \mid (x - x_0)$. Thus, there exists an integer n such that $x - x_0 = \frac{b}{d}n$ and thus, $x = x_0 + \frac{b}{d}n$. Plug this into the following:

$$\begin{aligned} \tfrac{a}{d}(x - x_0) &= \tfrac{-b}{d}(y - y_0) \\ \tfrac{a}{d} \cdot \tfrac{b}{d}n &= \tfrac{-b}{d}(y - y_0) \\ \tfrac{-a}{d}n &= y - y_0 \end{aligned}$$

Hence, $y = y_0 - \frac{a}{d}n$ completing the proof. ■

Instructor's Comments: Something to note about the proof. An argument using 'similarly' won't work above since you want to ensure that the n you get from doing the above (and the one you would get by arguing 'similarly') is the same.

Instructor's Comments: This is the 20 minute mark.

Example: Alice has a lot of mail to send. She wishes to spend exactly 100 dollars buying 49 cent and 53 cent stamps. In how many ways can she do this?

Solution: Let x be the number of 49 cent stamps. Let y be the number of 53 cent stamps. Note that $x, y \in \mathbb{Z}$ and that $x, y \geq 0$. We want to solve

$$\begin{aligned} 0.49x + 0.53y &= 100 \\ 49x + 53y &= 10000 \end{aligned}$$

x	y	r	q
0	1	53	0
1	0	49	0
-1	1	4	1
13	-12	1	12
*	*	0	4

We solve this using the Extended Euclidean Algorithm:

Therefore, $49(13) + 53(-12) = 1$. Hence, $49(130000) + 53(-120000) = 10000$. Thus, by LDET2, all solutions are given by

$$\begin{aligned} x &= 130000 - 53n \\ y &= -120000 + 49n \end{aligned}$$

for all $n \in \mathbb{Z}$. Now, to answer the question, we need to determine all the answers that make sense. Since x and y are physical quantities, we know that $x \geq 0$ and $y \geq 0$. The first condition gives

$$\begin{aligned} x &\geq 0 \\ 130000 - 53n &\geq 0 \\ 2452 + \frac{44}{53} = \frac{130000}{53} &\geq n \end{aligned}$$

whereas the second condition gives

$$\begin{aligned} y &\geq 0 \\ -120000 + 49n &\geq 0 \\ n &\geq \frac{120000}{49} = 2448 + \frac{48}{49} \end{aligned}$$

Since $n \in \mathbb{Z}$, we see that $2449 \leq n \leq 2452$. Thus there are 4 possible solutions. ■

Instructor's Comments: Watch for the off by one error! This is the 30-35 minute mark

Handout or Document Camera or Class Exercise

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

Solution: Dividing by 3 gives

$$5x - 8y = 3$$

By inspection, $x_0 = -1$ and $y_0 = -1$ is a solution. Since $\gcd(5, -8) = 1$, by LDET2 we have that the complete solution set is given by

$$\begin{aligned} x &= -1 - (-8)n = -1 + 8n \\ y &= -1 + 5n \end{aligned}$$

for all $n \in \mathbb{Z}$. By the statement,

$$\begin{aligned} 0 \leq \quad & x \quad \leq 20 \\ 0 \leq -1 + & 8n \leq 20 \\ 1 \leq \quad & 8n \quad \leq 21 \end{aligned}$$

Giving $n = 1, 2$ and

$$\begin{aligned} 0 \leq \quad & y \quad \leq 20 \\ 0 \leq -1 + & 5n \leq 20 \\ 1 \leq \quad & 5n \quad \leq 21 \end{aligned}$$

giving $n = 1, 2, 3, 4$. Hence the overlap of $n = 1$ or $n = 2$ gives all solutions. These are given by $(7, 4)$ and $(15, 9)$. ■

Instructor's Comments: This is the 40-45 minute mark.

Instructor's Comments: This last page is to motivate the switch to congruences. This is where the number theory really kicks off. If you get the opportunity to, mention the definition of congruences. Seeing this definition once or twice is really useful. Students should be told to commit this to memory quickly otherwise these next two weeks will seem unnecessarily difficult.

Congruences

Idea: Simplify problems in divisibility.

(i) Is 156723 divisible by 11?

(ii) What angle do you get after a 1240 degree rotation?

(iii) What time is it 400 hours from now?

Note: We only care about the above values up to multiples of 11, 360 and 24.

Definition: Let $m \in \mathbb{N}$. We say that two integers a and b are congruent modulo m if and only if $m \mid (a-b)$ and we write $a \equiv b \pmod{m}$. If $m \nmid (a-b)$, we write $a \not\equiv b \pmod{m}$.

Instructor's Comments: It's important enough to mention again - commit the previous definition to memory!!!

Example:

$$7 \equiv 4 \pmod{3}$$
$$4 \equiv 7 \pmod{3}$$
$$4 \equiv 4 \pmod{3}$$
$$7 \not\equiv 4 \pmod{4}$$
$$10 \equiv 15 \pmod{5}$$
$$15 \equiv 30 \pmod{5}$$
$$10 \equiv 30 \pmod{5}$$

Lecture 25

Instructor's Comments: First part is to recall the definition of congruence. This is extremely important. Get students to do this on their own

Definition: Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then a is congruent to b modulo n if and only if $n \mid (a - b)$ and we write $a \equiv b \pmod{n}$. This is equivalent to saying there exists an integer k such that $a - b = kn$ or $a = b + kn$.

Instructor's Comments: This is the 5 minute mark

Handout or Document Camera or Class Exercise

Instructor's Comments: Write on the board and get students to prove. These are follow your nose proofs

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 $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Proof:

(i) Since $n \mid 0 = (a - a)$, we have that $a \equiv a \pmod{n}$.

(ii) Since $n \mid (a - b)$, there exists an integer k such that $nk = (a - b)$. This implies that $n(-k) = b - a$ and hence $n \mid (b - a)$ giving $b \equiv a \pmod{n}$.

(iii) Since $n \mid (a - b)$ and $n \mid (b - c)$, by Divisibility of Integer Combinations, $n \mid ((a - b) + (b - c))$. Thus $n \mid (a - c)$ and hence $a \equiv c \pmod{n}$

Instructor's Comments: This is the 20 minute mark

Example: Without a calculator, determine if $167 \equiv 2015 \pmod{4}$ is true.

Solution: Since $2015 \equiv 3 \pmod{4}$ (valid as $4 \mid 2012 = 2015 - 3$) and $167 \equiv 3 \pmod{4}$ (valid as $4 \mid 164 = 167 - 3$), we see by symmetry that $3 \equiv 2015 \pmod{4}$ and hence by transitivity that $167 \equiv 2015 \pmod{4}$.

Alternate Solution: Does $4 \mid (2015 - 167) = 1848$?

Instructor's Comments: This is the 25 minute mark

Handout or Document Camera or Class Exercise

Instructor's Comments: Write on board and get students to prove on their own

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

Proof:

(i) Since $m \mid (a - a')$ and $n \mid (b - b')$, we have by Divisibility of Integer Combinations $m \mid (a - a' + (b - b'))$. Hence $m \mid ((a + b) - (a' + b'))$ and so $a + b \equiv a' + b' \pmod{m}$.

(ii) Since $m \mid (a - a')$ and $n \mid (b - b')$, we have by Divisibility of Integer Combinations $m \mid (a - a' - (b - b'))$. Hence $m \mid ((a - b) - (a' - b'))$ and so $a - b \equiv a' - b' \pmod{m}$.

(iii) Since $m \mid (a - a')$ and $n \mid (b - b')$, we have by Divisibility of Integer Combinations $m \mid ((a - a')b + (b - b')a')$. Hence $m \mid ab - a'b'$ and so $ab \equiv a'b' \pmod{m}$.

Instructor's Comments: This is the 40 minute mark

Corollary If $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$ for $k \in \mathbb{N}$.

Example: Since $2 \equiv 6 \pmod{4}$, we have that
$2^2 \equiv 6^2 \pmod{4}$, that is, $4 \equiv 36 \pmod{4}$.

Example: Is $5^9 + 62^{2000} - 14$ divisible by 7?

Solution: Reduce modulo 7. By Properties of Congruence, we have

$$\begin{aligned} 5^9 + 62^{2000} - 14 &\equiv (-2)^9 + (-1)^{2000} - 0 \pmod{7} \\ &\equiv -2^9 + 1 \pmod{7} \\ &\equiv -(2^3)^3 + 1 \pmod{7} \\ &\equiv -(8)^3 + 1 \pmod{7} \\ &\equiv -(1)^3 + 1 \pmod{7} \\ &\equiv 0 \pmod{7} \end{aligned}$$

Therefore, the number is divisible by 7.

Instructor's Comments: This is the 50 minute mark. Some things to note above: In computations, we often don't cite every single time a basic proposition is used like PC or CER or the major corollary above. Be sure though while explaining to mention the use of the corollary above.

Lecture 26

Leading Question: Is 98654320480 divisible by 120?

Instructor's Comments: Note that $120 = 5!$

Divisibility Rules

A positive integer n is divisible by

A) 2^k if and only if the last k digits are divisible by 2^k where $k \in \mathbb{N}$.

B) 3 (or 9) if and only if the sum of the digits is divisible by 3 (or 9).

C) 5^k if and only if the last k digits are divisible by 5^k where $k \in \mathbb{N}$.

D) 7 (or 11 or 13) if and only if the alternating sum of triples of digits is divisible by 7 (or 11 or 13).

Example: $n = 123456333$. Look at $333 - 456 + 123 = 0$ Since $7 \mid 0$ (and 11 and 13), we see that $7 \mid n$ (and 11 and 13).

We prove that 9 divides a number n if and only if the sum of the digits is divisible by 9.

Proof: Let $n \in \mathbb{N}$. Write

$$n = d_0 + 10d_1 + 10^2 d_2 + ... + 10^k d_k$$

where $d_i \in \{0, 1, 2, ..., 9\}$. (For example, $213 = 3 + 10(1) + 100(2)$). Thus,

$$\begin{aligned} 9 \mid n &\Leftrightarrow n \equiv 0 \pmod 9 \\ &\Leftrightarrow 0 \equiv d_0 + 10d_1 + ... + 10^k d_k \pmod 9 \\ &\Leftrightarrow 0 \equiv d_0 + d_1 + ... + d_k \pmod 9 \qquad \text{By (PC)} \\ &\Leftrightarrow 9 \mid (d_0 + d_1 + ... + d_k) \end{aligned}$$

Hence $9 \mid n$ if and only if 9 divides the sum of the digits of n. ■

Instructor's Comments: Note this is the first time I used an iff bidirectional proof. If this is your first time too you should make a note. This is the 10-15 minute mark. Note that if you're running low on time you needn't write out all the divisibility rules (or even mention them!)

Let's look at some examples of division of congruences. Can I divide integers with congruences?

(i) $3 \equiv 24 \pmod 7$

(ii) $1 \equiv 8 \pmod 7$

(iii) $3 \equiv 27 \pmod 6$

(iv) $1 \not\equiv 9 \pmod 6$

The above examples suggests that if you're dividing by a number that is coprime to the modulus, then you can divide. This is true in general.

Proposition: (Congruences and Division (CD)). Let $a, b, c \in \mathbb{Z}$ and let $n \in \mathbb{N}$. If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

Proof: By assumption, $n \mid (ac - bc)$ so $n \mid c(a - b)$. Since $\gcd(c, n) = 1$, by Coprimeness and Divisibility, $n \mid (a - b)$. Hence $a \equiv b \pmod{n}$.

Instructor's Comments: This is the 20-25 minute mark. introduce the next proposition as something they know but helps organize thoughts.

Proposition: (Congruent iff Same Remainder - CISR) Let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder after division by n.

Instructor's Comments: Delay the proof until after they get a chance to use it.

What is the remainder when $77^{100}(999) - 6^{83}$ is divided by 4?

Solution: Notice that

$$6 = 4(1) + 2 \qquad 77 = 19(4) + 1 \qquad 999 = 249(4) + 3$$

Hence, by Congruent if and only if Same Remainder, we have $77 \equiv 1 \pmod 4$ and $999 \equiv 3 \pmod 4$. Thus, by Properties of Congruences,

$$\begin{aligned} 77^{100}(999) - 6^{83} &\equiv (1)^{100}(3) - 2^{83} \pmod 4 \\ &\equiv 3 - 2^2 \cdot 2^{81} \pmod 4 \\ &\equiv 3 - 4 \cdot 2^{81} \pmod 4 \\ &\equiv 3 - 0(2^{81}) \pmod 4 \\ &\equiv 3 \pmod 4 \end{aligned}$$

Once again by Congruent If and only If Same Remainder, 3 is the remainder when $77^{100}(999) - 6^{83}$ is divided by 4. ■

Restating,

Proposition: (Congruent iff Same Remainder - CISR) Let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder after division by n.

Proof: By the Division Algorithm, write $a = nq_a + r_a$ and $b = nq_b + r_b$ where $0 \leq r_a, r_b < n$. Subtracting gives

$$a - b = n(q_a - q_b) + r_a - r_b$$

To prove $\Rightarrow$, first assume that $a \equiv b \pmod{n}$, that is $n \mid a - b$. Since $n \mid n(q_a - q_b)$, we have by Divisibility of Integer Combinations that $n \mid (a - b) + n(q_a - q_b)(-1)$ and thus, $n \mid r_a - r_b$. By our restriction on the remainders, we see that the difference is bounded by

$$-n + 1 \leq r_a - r_b \leq n - 1$$

However, only 0 is divisible by n in this range! Since $n \mid (r_a - r_b)$, we must have that $r_a - r_b = 0$. Hence $r_a = r_b$.

$\Leftarrow$ Assume that $r_a = r_b$. Since

$$a - b = n(q_a - q_b) + r_a - r_b = n(q_a - q_b)$$

we see that $n \mid (a - b)$ and hence $a \equiv b \pmod{n}$. ■

Instructor's Comments: This is likely the 50 minute mark. If it isn't get students to work or think about the following problem which you'll take up in the next class.

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

Lecture 27

Instructor's Comments: An important announcement. Students should probably read the textbook but I anticipate most don't just due to timing restrictions. However, I would strongly advise students read Chapter 26 to get practice with the plethora of notation.

Handout or Document Camera or Class Exercise

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

Solution: Want the remainder when we divide by 10. Hence reduce modulo 10 and use Congruent If and Only If Same Remainder.

$$\begin{aligned} 5^{32} \cdot 3^{10} + 9^{22} &\equiv (5^2)^{16} \cdot 9^5 + (-1)^{22} \pmod{10} \\ &\equiv 5^{16}(-1)^5 + 1 \pmod{10} \\ &\equiv (5^2)^8(-1) + 1 \pmod{10} \\ &\equiv -5^8 + 1 \pmod{10} \\ &\equiv -(5^2)^4 + 1 \pmod{10} \\ &\equiv -5^4 + 1 \pmod{10} \\ &\equiv -625 + 1 \pmod{10} \\ &\equiv -4 \pmod{10} \\ &\equiv 6 \pmod{10} \end{aligned}$$

Hence the last digit is 6. ■

Instructor's Comments: This is the 10 minute mark.

Linear Congruences

Question: Solve $ax \equiv c \pmod{m}$ where $a, c \in \mathbb{Z}$ and $m \in \mathbb{N}$ for $x \in \mathbb{Z}$.

Note: when we are solving $ax = c$ over the integers, we know that this has a solution if and only if $a \mid c$.

Example: Solve $4x \equiv 5 \pmod{8}$.

Solution: We associate a linear Diophantine equation to this linear congruence. By definition, there exists a $z \in \mathbb{Z}$ such that $4x - 5 = 8z$, that is, $4x - 8z = 5$. Now, letting $y = -z$. gives the linear Diophantine equation

$$4x + 8y = 5$$

Instructor's Comments: From now on I will jump straight to this version of the LDE without mentioning it so make sure they understand this change of variables trick to translate to an LDE quickly. This is why I go through this here.

Since $\gcd(4, 8) = 4 \nmid 5$, by LDET1, we see that this LDE has no solution. Hence the original congruence has no solutions. ■

Solution 2: Let $x \in \mathbb{Z}$. By the Division Algorithm, $x = 8q + r$ for some $0 \leq r \leq 7$ and q, r integers. By Congruent If and Only If Same Remainder, $4x \equiv 5 \pmod{8}$ holds if and only if $4r \equiv 5 \pmod{8}$. Thus, if we can prove that no number from $0 \leq x \leq 7$ works, then no integer x can satisfy the congruence.

Instructor's Comments: Again make a note that this explanation is not needed anymore to do these problems and is included here only for clarity.

Trying the possibilities

$$\begin{aligned}
4(0) &\equiv 0 \pmod{8} \\
4(1) &\equiv 4 \pmod{8} \\
4(2) &\equiv 0 \pmod{8} \\
4(3) &\equiv 4 \pmod{8} \\
4(4) &\equiv 0 \pmod{8} \\
4(5) &\equiv 4 \pmod{8} \\
4(6) &\equiv 0 \pmod{8} \\
4(7) &\equiv 4 \pmod{8}
\end{aligned}$$

shows that $4x \equiv 5 \pmod{8}$ has no solution. ■

Solution 3: Assume towards a contradiction that there exists an integer x such that $4x \equiv 5 \pmod{8}$. Multiply both sides by 2 to get (by Properties of Congruence) that

$$0 \equiv 0x \equiv 8x \equiv 10 \pmod{8}$$

Hence, $8 \mid 10$ however $8 \nmid 10$. This is a contradiction. Thus, there are no integer solutions to $4x \equiv 5 \pmod{8}$. ■

Instructor's Comments: This is the 25 minute mark. Take your time with the previous argument. Encourage students to be creative with how they argue! If they find a solution encourage them to find another!

Example: $5x \equiv 3 \pmod{7}$.

Solution: Look Modulo 7. Then there are only 7 possibilities to consider for x. Trying them gives

$$\begin{aligned}
5(0) &\equiv 0 \pmod{7} \\
5(1) &\equiv 5 \pmod{7} \\
5(2) &\equiv 3 \pmod{7} \\
5(3) &\equiv 1 \pmod{7} \\
5(4) &\equiv 6 \pmod{7} \\
5(5) &\equiv 4 \pmod{7} \\
5(6) &\equiv 2 \pmod{7}
\end{aligned}$$

Therefore, $x \equiv 2 \pmod{7}$ gives the complete set of solutions. ■

Solution 2: This is equivalent to solving the LDE

$$5x + 7y = 3$$

A solution is given by $(x, y) = (2, -1)$. By LDET2, $x = 2 + 7n$ and $y = -1 + 5n$ for all n gives the complete set of solutions. Hence $x \equiv 2 \pmod{7}$ gives the complete solutions. ■

Solution 3: $5x \equiv 3 \pmod{7} \Leftrightarrow x \equiv 2 \pmod{7}$. We see this by multiplying by 5 to go in reverse and multiplying by 3 to go from the left to the right. Something like:

$$\begin{aligned}
5x &\equiv 3 \pmod{7} \\
(3)5x &\equiv (3)3 \pmod{7} \\
15x &\equiv 9 \pmod{7} \\
x &\equiv 2 \pmod{7}
\end{aligned}$$

and multiply by 3 to go in reverse.

Instructor's Comments: Mention that this is related to something called finding an inverse for 5.

Example: $2x \equiv 4 \pmod{6}$.

Solution: Trying all 6 possibilities yields,

$$\begin{aligned}
2(0) &\equiv 0 \pmod{6} \\
2(1) &\equiv 2 \pmod{6} \\
2(2) &\equiv 4 \pmod{6} \\
2(3) &\equiv 0 \pmod{6} \\
2(4) &\equiv 2 \pmod{6} \\
2(5) &\equiv 4 \pmod{6}
\end{aligned}$$

Hence, $x \equiv 2, 5 \pmod 6$ give solutions. These solutions are captured by $x \equiv 2 \pmod 3$. (It is not a coincidence that $3 = 6/\gcd(2, 4)$). ■

Instructor's Comments: Try to make this the 35 minute mark.

Summarizing the above give the following theorem:

Theorem: LCT1 (Linear Congruence Theorem 1). Let $a, c \in \mathbb{Z}$ and $m \in \mathbb{N}$ and $\gcd(a, m) = d$. Then $ax \equiv c \pmod m$ has a solution if and only if $d \mid c$. Further, we have d solutions modulo m and 1 solution modulo m/d. Moreover, if $x = x_0$ is a solution, then $x \equiv x_0 \pmod{m/d}$ forms the complete solution set or alternatively, $x = x_0 + \frac{m}{d}n$ for all $n \in \mathbb{Z}$ or for another alternative way to write the solution:

$$x \equiv x_0, x_0 + \tfrac{m}{d}, x_0 + 2\tfrac{m}{d}, ..., x_0 + (d-1)\tfrac{m}{d} \pmod m$$

Proof: Read p. 180. ■

Instructor's Comments: This is the 40-45 minute mark.

Handout or Document Camera or Class Exercise

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

Solution: Notice that $9(4) = 36 \equiv 6 \pmod{15}$. Hence, by LCT1, all solutions are given by $x \equiv 4 \pmod{15/\gcd(9,15)}$, or $x \equiv 4 \pmod{5}$. This is equivalent to $x \equiv 4, 9, 14 \pmod{15}$.

Alternate Solution: Equivalent to solving the LDE

$$\begin{aligned} & 9x + 15y = 6 \\ \implies & 3x + 5y = 2 \end{aligned}$$

By LDET2, since $(x, y) = (-1, 1)$ is a solution, all solutions are given by

$$\begin{aligned} x &= -1 + 5n \\ y &= 1 - 3n \end{aligned}$$

for all $n \in \mathbb{Z}$. Therefore, a solution is given by $x \equiv -1 \pmod{5}$ or $x \equiv 4 \pmod{5}$. Equivalently, $x \equiv 4, 9, 14 \pmod{15}$.

Instructor's Comments: This is the 50 minute mark.

Lecture 28

Handout or Document Camera or Class Exercise

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

Solution:

A) $x = 173 \equiv 3 \pmod{17}$

B) $x = 15^5 + 19^3 - 4 \equiv (-2)^5 + 2^3 - 4 \equiv -32 + 8 - 4 \equiv 2 + 4 \equiv 6 \pmod{17}$

C) $x = 5 \cdot 18^{100} \equiv 5(1)^{100} \equiv 5 \pmod{17}$

D) $x = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \equiv 6 \cdot 35 \cdot (-6)(-4) \equiv 6 \cdot 1 \cdot 24 \equiv 6 \cdot 7 \equiv 42 \equiv 8 \pmod{17}$

E) $x = 17^0 + 17^1 + 17^2 + 17^3 + 17^4 + 17^5 + 17^6 \equiv 1 \pmod{17}$

Answer is the second option since $x \equiv 40 \equiv 6 \pmod{17}$.

Instructor's Comments: This is the 5-10 minute mark

Instructor's Comments: Try to make the next exercise only take you to the 10 minute mark.

Example: Show that there are no integer solutions to $x^2 + 4y = 2$.

Proof: Assume towards a contradiction that there exist integers x and y such that $x^2 + 4y = 2$. Reducing modulo 4 yields $x^2 \equiv 2 \pmod 4$. Trying all the possibilities yields

$$(0)^2 \equiv 0 \pmod 4$$
$$(1)^2 \equiv 1 \pmod 4$$
$$(2)^2 \equiv 0 \pmod 4$$
$$(3)^2 \equiv 1 \pmod 4$$

Hence there are no integer solutions. ■

Note: Notice that sometimes, you end up with many solutions. For example, $x^2 \equiv 1 \pmod 8$ has 4 solutions (all the odd numbers work! This is an exercise to check)

Instructor's Comments: Now comes what I think is the hardest to grasp concept in this course; the abstraction of Z/mZ. I personally am going to discuss rings here and take a bit more time here to save a bit of time later on in the course. I will introduce the notion of a ring and field here so that when we get to complex numbers, it will go a bit quicker. This will cause me to spend more time here on topics but I think that's okay.

$\mathbb{Z}_m$ or $\mathbb{Z}/m\mathbb{Z}$ The integers modulo m

Definition: The congruence or equivalence class modulo m of an integer a is the set of integers

$$[a] := \{x \in \mathbb{Z} : x \equiv a \pmod m\}$$

Note: $:=$ means "defined as".

Further, define

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} := \{[0], [1], ..., [m-1]\}$$

Definition: A commutative ring is a set R along with two closed operations $+$ and $\cdot$ such that for $a, b, c \in R$ and

(i) Associative $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

(ii) Commutative $a + b = b + a$ and $ab = ba$.

(iii) Identities: there are [distinct] elements $0, 1 \in R$ such that $a + 0 = a$ and $a \cdot 1 = a$.

(iv) Additive inverses: There exists an element $-a$ such that $a + (-a) = 0$.

(v) Distributive Property $a(b + c) = ab + ac$.

Example: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Not $\mathbb{N}$

Definition: If in addition, every nonzero element has a multiplicative inverse, that is an element a^{-1} such that $a \cdot a^{-1} = 1$, we say that R is a field.

Example: $\mathbb{Q}$, $\mathbb{R}$. Not $\mathbb{N}$ or $\mathbb{Z}$.

Instructor's Comments: This should take you tot he 25-30 minute mark

Definition: We make $\mathbb{Z}_m$ a ring by defining addition and subtraction and multiplication by $[a] \pm [b] := [a \pm b]$ and $[a] \cdot [b] := [ab]$. This makes $[0]$ the additive identity and $[1]$ the multiplicative identity.

Instructor's Comments: Note that the $[a+b]$ means add then reduce modulo m. There is something subtle going on here that might be lost on students.

There is one issue we need to resolve here; the issue of being well defined. How do we know that the above definition does not depend on the representatives chosen for $[a]$ and $[b]$?

Example: For example, in $\mathbb{Z}_6$, is it true that $[2][5] = [14][-13]$?

Instructor's Comments: Note that $[2] = [14]$ and $[5] = [-13]$. To properly prove well-definedness, you would have to do this for all possible representations of $[a]$. Since this will create a notational disaster, I think it's best to try to illustrate the point with a concrete example.

Proof: Note that in $\mathbb{Z}_6$, we have

$$\text{LHS} = [2][5] = [2 \cdot 5] = [10] = [4]$$

and also

$$\text{RHS} = [14][-13] = [14(-13)] = [-182] = [-2] = [4]$$

completing the proof. ■

Definition: The members $[0], [1], ..., [m-1]$ are sometimes called representative members.

Instructor's Comments: Minimum this is the 35 minute mark.

Instructor's Comments: In practice, this was the 50 minute mark but either way that's okay - hopefully you can squeeze in the addition table.

Addition table for $\mathbb{Z}_4$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Lecture 29

Handout or Document Camera or Class Exercise

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.

Instructor's Comments: Note to "properly" prove these, you would have to prove these as an equality of sets.

Solution:

(i) $[75] - [x] = [50]$ is equivalent to solving $75 - x \equiv 50 \pmod{14}$. Solving here gives $x \equiv 25 \equiv 11 \pmod{14}$.

(ii) $[10][x] = [1]$ is equivalent to solving $10x \equiv 1 \pmod{14}$. Since $\gcd(10, 14) = 2 \nmid 1$, we see by LCT1 that this has no solution.

(iii) $[10][x] = [2]$ is equivalent to solving $10x \equiv 2 \pmod{14}$. Notice that $x = 3$ is a solution and so by LCT1, we see that $x \equiv 3 \pmod{14/\gcd(2, 14)}$ gives a complete solution. This is the same as $x \equiv 3 \pmod{7}$ or $x \equiv 3, 10 \pmod{14}$ or $x = [3], [10]$.

Instructor's Comments: This is the 10 minute mark. The last point that $x \equiv 3 \pmod{7}$ and $x \equiv 3, 10 \pmod{14}$ are equivalent is lost on some students. Remind them that the first meant $x = 3 + 7k$ and that k has two options - being even (which is equivalent to 3 modulo 14) or being odd (which is equivalent to 10 modulo 14). A similar argument can be applied if it were say 7 to 21 etc.

Instructor's Comments: If you want an extra problem with congruences, try Solve $[15][x] + [7] = [12]$ in $\mathbb{Z}_{10}$. Otherwise mention this later.

Inverses

(i) $[-a]$ is the additive inverse of $[a]$, that is, $[a] + [-a] = [0]$.

(ii) If there exists an element $[b] \in \mathbb{Z}_m$ such that $[a][b] = [1] = [b][a]$, we call $[b]$ the multiplicative inverse of $[a]$ and write $[b] = [a]^{-1}$ or $b \equiv a^{-1} \pmod{m}$.

Example: $[5][11] = [1]$ in $\mathbb{Z}_{18}$. Therefore, $[5]^{-1} = [11]$ and $[11]^{-1} = [5]$.

Note: WARNING Multiplicative inverses do not always exist!

Example: $[9][x] = [1]$ in $\mathbb{Z}_{18}$ has no solution. The left hand side is always $[0]$ or $[9]$ for every value of $[x]$. Hence $[9]^{-1}$ does not exist in $\mathbb{Z}_{18}$.

Instructor's Comments: This is the 15 minute mark

Handout or Document Camera or Class Exercise

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

Solution: Additive inverse: $[-7] = [4]$. For the multiplicative inverse, we want to solve

$$[7][x] = [1] \qquad \Leftrightarrow \qquad 7x \equiv 1 \pmod{11}$$

You can solve this by turning this into the LDE $7x + 11y = 1$ and solving that. However, because the numbers are small, guessing and checking is a far more efficient strategy. Notice that

$$7 \cdot 3 \equiv 21 \equiv 10 \equiv -1 \pmod{11}$$

Thus, $7(-3) \equiv 1 \pmod{11}$ and so $[x] = [-3] = [8]$ is the inverse of $[7]$ in $\mathbb{Z}_{11}$.

Instructor's Comments: This is the 25 minute mark

Proposition: Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$.

(i) $[a]^{-1}$ exists in $\mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$.

(ii) $[a]^{-1}$ is unique if it exists.

Proof:

(i)

$$\begin{aligned} [a]^{-1} \text{ exists} \quad &\Leftrightarrow \quad [a][x] = [1] \text{ is solvable in } \mathbb{Z}_m \\ &\Leftrightarrow \quad ax + my = 1 \text{ is a solvable LDE} \\ &\Leftrightarrow \quad \gcd(a, m) = 1 \text{ GCDOO} \end{aligned}$$

completing the proof. ■

(ii) Assume $[a]^{-1}$ exists. Suppose there exists a $[b] \in \mathbb{Z}_m$ such that $[a][b] = [1] = [b][a]$. Then

$$\begin{aligned} [a]^{-1}[a][b] &= [a]^{-1}[1] \\ [1][b] &= [a]^{-1} \\ [b] &= [a]^{-1} \end{aligned}$$

Instructor's Comments: This is the 35 minute mark

Exercise: Solve $[15][x] + [7] = [12]$ in $\mathbb{Z}_{10}$.

Instructor's Comments: Solution: This is equivalent to solving

$$15x + 7 \equiv 12 \pmod{10}.$$

Isolating for x gives

$$15x \equiv 5 \pmod{10}.$$

Since $15 \equiv 5 \pmod{10}$, Properties of Congruences states that

$$5x \equiv 5 \pmod{10}.$$

This clearly has the solution $x = 1$. Hence, by Linear Congruence Theorem 1, we have that

$$x \equiv 1 \pmod{\tfrac{10}{\gcd(5,10)}}$$

gives the complete set of solutions. Thus, $x \equiv 1 \pmod{2}$ or $x \equiv 1, 3, 5, 7, 9 \pmod{10}$. Since the original question is framed in terms of congruence classes, our answer should be as well and hence

$$[x] \in \{[1], [3], [5], [7], [9]\}.$$

For extra practice, see if you can phrase this argument using Linear Congruence Theorem 2.

Handout or Document Camera or Class Exercise

Instructor's Comments: This is a good time to introduce the notation TFAE

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

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

Instructor's Comments: This is the 40 minute mark

Instructor's Comments: This is the FLT part of the course. I think this proof is fantastic and really creative so I like doing it. One could of course prove FLT using induction and the binomial theorem, which I would say if you have in the course you should do. You can choose to not to the proof or maybe show why it's true for a specific prime but I like actually showing the proof. It's elegant clever and really just awesome. I recommend being brave and showing it. This proof will spill over to the next lecture. Keep shifting content until you reach the square and multiply algorithm which is optional material that you can afford to skip and catch up there.

Theorem: Fermat's Little Theorem (FℓT). If p is a prime number and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$. Equivalently, $[a^{p-1}] = [1]$ in $\mathbb{Z}_p$.

Example:

(i) $5^6 \equiv 1 \pmod{7}$

(ii) $4^6 \equiv 1 \pmod{7}$

(iii) $39^6 \equiv 1 \pmod{7}$

Note: $p-1$ is in the exponent and not the base. For example, $(5-1)^3 \equiv 4 \pmod{5}$.

Note: $p-1$ is not necessarily the smallest exponent such that $a^k \equiv 1 \pmod{p}$. For example $6^2 \equiv 1 \pmod{7}$.

Lemma: Let $\gcd(a,p) = 1$. Let

$$S := \{a, 2a, ..., (p-1)a\} \qquad T := \{1, 2, ..., p-1\}.$$

Then the elements of S are unique modulo p and for all $s \in S$, there exists a unique element $t \in T$ such that $s \equiv t \pmod{p}$.

Proof: We first show that S contains $p-1$ distinct nonzero elements modulo p.

Let $ka, ma \in S$ with $1 \leq k, m \leq p-1$ integers. Now, if $ka \equiv ma \pmod{p}$, then $p \mid a(k-m)$. Since $\gcd(a,p) = 1$, we see that $p \mid (k-m)$ by Coprimeness and Divisibility. Since

$$-p < 2 - p \leq k - m \leq p - 2 < p$$

and $p \mid (k-m)$, we see that $k - m = 0$, that is, $k = m$. Lastly, if $ka \equiv 0 \pmod{p}$, then $p \mid ka$. By Euclid's Lemma, $p \mid k$, a contradiction since $1 \leq k \leq p-1$ and p is prime, or $p \mid a$ also a contradiction since $\gcd(a,p) = 1$. Thus, S has $p-1$ distinct nonzero elements modulo p.

So if $ka \in S$, then $ka \equiv n \pmod{p}$ for some $1 \leq n \leq p-1$ and this n is unique since if in addition $ka \equiv \ell \pmod{p}$ with $1 \leq \ell \leq p-1$, subtracting the two congruences gives $p \mid (n - \ell)$, a contradiction unless $\ell = n$ since

$$-p < 2 - p \leq \ell - n \leq p - 2 < p.$$

This completes the proof. ■

Proof: (of Fermat's Little Theorem). Using the lemma, valid since $p \nmid a$ holds if and only if $\gcd(a,p) = 1$ (by say GCDPF), we have that by the lemma S and T contain the same elements modulo p and hence their products must be congruent modulo p. Thus,

$$\prod_{x \in S} x \equiv \prod_{y \in T} y \pmod{p}$$
$$\prod_{k=1}^{p-1} ka \equiv \prod_{j=1}^{p-1} j \pmod{p}$$
$$a^{p-1} \prod_{k=1}^{p-1} k \equiv \prod_{j=1}^{p-1} j \pmod{p}$$

Let $Q = \prod_{j=1}^{p-1} j = (1)(2)...(p-1)$. Then

$$Qa^{p-1} \equiv Q \pmod{p}$$

Since $\gcd(Q,p) = 1$ (as Q is a product of numbers less than a prime p), we have that Q^{-1} exists and hence

$$Q^{-1}Qa^{p-1} \equiv Q^{-1}Q \pmod{p}$$

and thus $a^{p-1} \equiv 1 \pmod{p}$ completing the proof . ■

Instructor's Comments: This is the 50 minute mark. It's a bit of an intense proof but really cool.

Lecture 30

Handout or Document Camera or Class Exercise

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

Solution: Recall (FℓT): If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ where p is a prime.

By FℓT,

$$\begin{aligned} 7^{10} &\equiv 1 \pmod{11} \\ 7^{90} &\equiv 1 \pmod{11} && \text{Raise both sides to the power of 9} \\ 7^{92} &\equiv 7^2 \equiv 49 \equiv 5 \pmod{11} \end{aligned}$$

Alternatively,

$$\begin{aligned} 7^{92} &\equiv 7^{9(10)+2} \pmod{11} \\ &\equiv (7^{10})^9 7^2 \pmod{11} \\ &\equiv 1^9 \cdot 7^2 \pmod{11} && \text{By F}\ell\text{T since } 11 \nmid 7 \\ &\equiv 49 \pmod{11} \\ &\equiv 5 \pmod{11} \end{aligned}$$

completing the question. ■

Instructor's Comments: This is the 10 minute mark

Corollary: If p is a prime and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.

Proof: If $p \mid a$, then $a \equiv 0 \pmod{p}$. This implies that $a^p \equiv 0 \equiv a \pmod{p}$.

If $p \nmid a$, then by FℓT, $a^{p-1} \equiv 1 \pmod{p}$ and hence $a^p \equiv a \pmod{p}$ completing the proof. ■

Corollary: If p is a prime number and $[a] \neq [0]$ in $\mathbb{Z}_p$, then there exists a $[b] \in \mathbb{Z}_p$ such that $[a][b] = [1]$.

Proof: Since $[a] \neq [0]$, we see that $p \nmid a$. Hence by FℓT, $a^{p-1} \equiv 1 \pmod{p}$ and thus $a \cdot a^{p-2} \equiv 1 \pmod{p}$. This is sensible since $p - 2 \geq 0$. Thus, take $[b] = [a^{p-2}]$. ■

Instructor's Comments: Students should be able to do the next one - give them a shot at it on their own first! There's a handout one that depends on this so it might be good to get them thinking.

Corollary: If $r = s + kp$, then $a^r \equiv a^{s+k} \pmod{p}$ where p is a prime and $a \in \mathbb{Z}$ and $r, s, k \in \mathbb{N}$.

Instructor's Comments: It should be noted that here we want r, s, k to be at least nonnegative. We haven't really talked about what it means to take a^k when $k < 0$ except for $k = -1$. It's not hard but in this corollary, the important fact is that a might not be invertible so things like a^{-3} don't make sense necessarily.

Proof: We have

$$\begin{aligned} a^r &\equiv a^{s+kp} \pmod{p} \\ &\equiv a^s (a^p)^k \pmod{p} \\ &\equiv a^s (a)^k \pmod{p} && \text{By corollary to F}\ell\text{T} \\ &\equiv a^{s+k} \pmod{p} \end{aligned}$$

Instructor's Comments: This is the 20 minute mark.

Handout or Document Camera or Class Exercise

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 $r, s \in \mathbb{Z}$.

Solution: Since $r \equiv s \pmod{(p-1)}$, we have that $(p-1) \mid (r-s)$. Thus, there exists a $k \in \mathbb{Z}$ such that $(p-1)k = r - s$. Hence $r = s + (p-1)k$. Thus,

$$\begin{aligned} a^r &\equiv a^{s+(p-1)k} \pmod{p} \\ &\equiv a^s (a^{p-1})^k \pmod{p} \\ &\equiv a^s (1)^k \pmod{p} && \text{By F}\ell\text{T since } p \nmid a \\ &\equiv a^s \pmod{p}. \end{aligned}$$

This completes the proof. ■

Instructor's Comments: This is the 30 minute mark

Chinese Remainder Theorem (CRT)

Solve

$$x \equiv 2 \pmod 7$$
$$x \equiv 7 \pmod{11}$$

Instructor's Comments: Note to students this is the first time they are seeing two congruences with different moduli.

Using the first condition, write $x = 2 + 7k$ for some $k \in \mathbb{Z}$. Plugging into the second condition gives

$$2 + 7k \equiv 7 \pmod{11}$$
$$7k \equiv 5 \pmod{11}$$

Now there are a few ways to proceed. One could guess and check the inverse of 7. With this approach, we see that multiplying both sides by 3 gives

$$3 \cdot 7k \equiv 15 \pmod{11}$$
$$21k \equiv 4 \pmod{11}$$
$$-k \equiv 4 \pmod{11}$$
$$k \equiv -4 \pmod{11}$$
$$k \equiv 7 \pmod{11}$$

Therefore, $k = 7 + 11\ell$ for some $\ell \in \mathbb{Z}$. Alternatively, one can use the LDE approach on $7k + 11y = 5$ and use the Extended Euclidean Algorithm:

k	y	r	q
0	1	11	0
1	0	7	0
-1	1	4	1
2	-1	3	1
-3	2	1	1
		0	3

Hence $7(-3) + 11(2) = 1$ and thus $7(-15) + 11(10) = 5$. So by LDET2, we have that $k = -15 + 11n$ for all $n \in \mathbb{Z}$. Thus $k \equiv -15 \equiv 7 \pmod{11}$ and as above $k = 7 + 11\ell$ for some $\ell \in \mathbb{Z}$.

Instructor's Comments: Note here that to find all solution we need to use for all $n \in \mathbb{Z}$. Because out specific k is fixed however, we us for some at the end. What's happened here is that we've overloaded the use of k - once in the question but once in the LDE question process. This isn't a big deal and probably isn't worth mentioning unless a student asks.

Thus, since $x = 2 + 7k$ and $k = 7 + 11\ell$, we have

$$\begin{aligned} x &= 2 + 7k \\ &= 2 + 7(7 + 11\ell) \\ &= 51 + 77\ell \end{aligned}$$

Therefore, $x \equiv 51 \pmod{77}$ is the solution. ■

Instructor's Comments: This might take you to the 50 minute mark. Otherwise state the slide on the next lecture.

Lecture 31

Handout or Document Camera or Class Exercise

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

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

Instructor's Comments: This is the 5 minute mark. Remark that the statement of CRT is not nearly as useful as understanding the proof.

Example: Solve

$$\begin{aligned} x &\equiv 5 \pmod 6 \\ x &\equiv 2 \pmod 7 \\ x &\equiv 3 \pmod{11} \end{aligned}$$

From the first equation, $x = 5 + 6k$ for some $k \in \mathbb{Z}$. Plug this into the second equation gives

$$\begin{aligned} 5 + 6k &\equiv 2 \pmod 7 \\ 6k &\equiv -3 \pmod 7 \\ -k &\equiv -3 \pmod 7 \\ k &\equiv 3 \pmod 7 \end{aligned}$$

and hence $k = 3 + 7\ell$ for some $\ell \in \mathbb{Z}$. Therefore, $x = 5 + 6(3 + 7\ell) = 23 + 42\ell$. Therefore $x \equiv 23 \pmod{42}$. Now, we need to satisfy

$$\begin{aligned} x &\equiv 23 \pmod{42} \\ x &\equiv 3 \pmod{11} \end{aligned}$$

Instructor's Comments: This is done so that students can see the reduction pattern that emerges.

Since $x = 23 + 42\ell$, plugging this into the final equation gives

$$\begin{aligned} 23 + 42\ell &\equiv 3 \pmod{11} \\ -2\ell &\equiv -20 \pmod{11} \\ \ell &\equiv 10 \pmod{11} \end{aligned}$$

By Congruences and Divisibility [CD] valid since $\gcd(-2, 11) = 1$

Hence, $\ell = 10 + 11m$ for some $m \in \mathbb{Z}$. Combining gives

$$x = 23 + 42\ell = 23 + 42(10 + 11m) = 443 + 462m$$

Therefore, $x \equiv 442 \pmod{462}$.

Instructor's Comments: This is the 20 minute mark.

Some twists to Chinese Remainder Problems: Example: Solve

$$\begin{aligned} 3x &\equiv 2 \pmod 5 \\ 2x &\equiv 6 \pmod 7 \end{aligned}$$

Instructor's Comments: The twist here is that the left hand sides are not just x but they have a coefficient.

Solution: Treat each congruence separately and solve using Linear Congruence Theorem 1 (LCT1). By inspection $x = 4$ solves the first congruence (could also use Linear Diophantine Equation techniques). Hence by LCT1, $x \equiv 4 \pmod{5/\gcd(3,5)}$ or $x \equiv 4 \pmod 5$. Similarly, notice that $x = 3$ is a solution to the second congruence. Hence by LCT1 again,

$x \equiv 3 \pmod{7/\gcd(2,7)}$. This is equivalent to $x \equiv 3 \pmod 7$. Thus, the above system is equivalent to solving

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

which can be solved like a typical Chinese Remainder Theorem problem.

Instructor's Comments: Don't do this in class - included only because I used to solve this this way.

Alternate Solution: Multiplying the first equation by 2 and the second equation by 4 gives

$$\begin{aligned} 6x &\equiv 4 \pmod 5 \\ 8x &\equiv 24 \pmod 7. \end{aligned}$$

Simplifying gives

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

Then proceed like a typical Chinese Remainder Theorem problem.

Example: Solve

$$\begin{aligned} x &\equiv 4 \pmod 6 \\ x &\equiv 2 \pmod 8 \end{aligned}$$

Instructor's Comments: The twist here is that the moduli are not coprime. Turns out that the engine that proves the Chinese Remainder Theorem is exactly what one needs to do here. Sometimes however there are no solutions and usually there are solutions but at a moduli smaller than the product.

Solution: Using the first equation gives $x = 4 + 6k$ for some $k \in \mathbb{Z}$. Plug this into the second equation gives

$$\begin{aligned} 4 + 6k &\equiv 2 \pmod 8 \\ 6k &\equiv -2 \pmod 8 \\ 6k &\equiv 6 \pmod 8 \end{aligned}$$

Now, note that $k = 1$ is definitely a solution. By LCT1, we have that

$$k \equiv 1 \pmod{8/(\gcd(6,8))}$$

gives all solution. Hence $k \equiv 1 \pmod 4$ and thus $k = 1 + 4\ell$ for some $\ell \in \mathbb{Z}$. Therefore,

$$x = 4 + 6(1 + 4\ell) = 10 + 24\ell$$

Therefore, $x \equiv 10 \pmod{24}$ gives the complete set of solutions.

Instructor's Comments: This is the 40 minute mark. Could even take your time and make this a full lecture if you wanted. We're reaching a catch up lecture if you have fallen behind.

Example: Solve $x^2 \equiv 34 \pmod{99}$.

This implies that $99 \mid (x^2-34)$. Note that $9 \mid 99$. Therefore $9 \mid (x^2-34)$ by transitivity, $x^2 \equiv 34 \pmod{9}$. Note further that $11 \mid 99$. Therefore, $11 \mid (x^2-34)$ by transitivity. this implies that

$$\begin{aligned} x^2 &\equiv 34 \pmod{11} \\ x^2 &\equiv 1 \pmod{11} \\ x^2 &\equiv \pm 1 \pmod{11} \end{aligned} \qquad \text{By trying all 11 possibilities}$$

Similarly, $x^2 \equiv 34 \equiv 7 \pmod{9}$ and so $x \equiv \pm 4 \pmod{9}$ (try all 9 possibilities).

This gives four systems of equations:

$$\begin{aligned} x &\equiv 1 \pmod{11} \\ x &\equiv 4 \pmod{9} \end{aligned} \qquad \begin{aligned} x &\equiv 1 \pmod{11} \\ x &\equiv -4 \pmod{9} \end{aligned}$$

$$\begin{aligned} x &\equiv -1 \pmod{11} \\ x &\equiv 4 \pmod{9} \end{aligned} \qquad \begin{aligned} x &\equiv -1 \pmod{11} \\ x &\equiv -4 \pmod{9} \end{aligned}$$

To finish solving this, we can use the Chinese Remainder Theorem 4 times to give the solutions

$$x \equiv 23, 32, 67, 76 \pmod{99}$$

This leads to the following theorem.

Theorem: Splitting the Modulus (SM) Let m and n be coprime positive integers. Then, for any integers x and a, we have

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv a \pmod{n} \end{aligned}$$

simultaneously if and only if $x \equiv a \pmod{mn}$.

Instructor's Comments: This is the 50 minute mark. If not, start the proof.

Lecture 32

Instructor's Comments: This is a make up lecture. You can choose to cover many extra problems if you wish or head towards cryptography. I will probably include the square and multiply algorithm at some point as an extra topic.

Handout or Document Camera or Class Exercise

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]

Solution: Note that

$$\begin{aligned} 53^{242} + 5^{-1} &\equiv 4^{242} + 3 \pmod 7 \\ &\equiv 4^2 \cdot 4^{240} + 3 \pmod 7 \\ &\equiv 2 \cdot (4^6)^{40} + 3 \pmod 7 \\ &\equiv 2 \cdot 1^{40} + 3 \pmod 7 \\ &\equiv 5 \end{aligned}$$

Instructor's Comments: This is the 5-7 minute mark.

Theorem: Splitting the Modulus (SM) Let m and n be coprime positive integers. Then, for any integers x and a, we have

$$x \equiv a \pmod{m}$$
$$x \equiv a \pmod{n}$$

simultaneously if and only if $x \equiv a \pmod{mn}$.

Proof: ($\Leftarrow$) Assume that $x \equiv a \pmod{mn}$. Then $mn \mid (x - a)$. Since $m \mid mn$, by transitivity, we have that $m \mid (x-a)$ and hence $x \equiv a \pmod{m}$. Similarly, $x \equiv a \pmod{n}$.

($\Rightarrow$) Assume that $x \equiv a \pmod{m}$ and $x \equiv a \pmod{n}$. Note that $x = a$ is a solution. Since $\gcd(m, n) = 1$, by the Chinese Remainder Theorem, $x \equiv a \pmod{mn}$ gives all solutions.

Instructor's Comments: This is the 15 minute mark.

Handout or Document Camera or Class Exercise

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

Solution: We want to solve $x^5 + x^3 + 2x^2 + 1 \equiv 0 \pmod 6$. By Splitting the Modulus, we see that

$$x^5 + x^3 + 2x^2 + 1 \equiv 0 \pmod 2$$
$$x^5 + x^3 + 2x^2 + 1 \equiv 0 \pmod 3$$

Using equation 1 and plugging in $x \equiv 0 \pmod 2$ and $x \equiv 1 \pmod 2$ gives in both cases that

$$x^5 + x^3 + 2x^2 + 1 \equiv 1 \pmod 2$$

Therefore, $x^5 + x^3 + 2x^2 + 1$ is never divisible by 6. ■

Instructor's Comments: This is the 25 minute mark. From here you can choose to do more practice and have a full lecture on Cryptography or just do a half lecture on cryptography.

Cryptography

Note: The practice/study of secure communication.

Alice wants to communicate with Bob and receive messages from Bob but Eve is listening to all the messages they send to each other.

Instructor's Comments: Include a picture

Alice needs to encrypt messages to Bob so that even if Eve can see them, she cannot read them. However Bob needs to be able to read them and so needs a way to decrypt them.

Note: A cryptosystem should not depend on the secrecy of the methods of encryption and decryption used (except for possibly secret keys). The method must be assumed to be known by all.

Private Key Cryptography

Agree before hand on a secret encryption and decryption key.

Instructor's Comments: Mention ASCII encryption. Break up messages into many chunks and send those chunks.

Example: Caesar Cipher. Map a plain text message M to a ciphertext (encrypted message) given by

$$C \equiv M + 3 \pmod{26}$$

where $0 \leq C \leq 26$. In this way, one can encrypt letters to new letters. This worked well for Caesar mainly because most soldiers could not read (so even an unencrypted message might not have been understood).

Example: $APPLE$ gets translated as a sequence of numbers $0, 15, 15, 11, 4$ then encrypted by adding 3 to get $3, 18, 18, 14, 7$ and then converted back to letters $DSSOH$.

Cons of Private Key Cryptography

(i) Tough to share private key before hand.

(ii) Too many private keys to store.

(iii) Difficult to communicate with strangers.

Public Key Cryptography

Analogy: Pad lock. A pad lock is easy to lock but difficult to unlock without the key. The main paradigm here is as follows:

(i) Alice produces a private key d and a public key e.

(ii) Bob uses the public key e to take a message M and encrypt it to some ciphertext C

(iii) Bob then sends C over an insecure channel to Alice.

(iv) Alice decrypts C to M using d.

Note:

(i) Encryption and decryption are inverses to each other.

(ii) d and e are different,

(iii) Only d is secret.

Instructor's Comments: This is the 40 minute mark - maybe the 50 minute mark

Question: What makes a problem hard?

Instructor's Comments: Something along the lines of the first thing you try doesn't work, a problem that has resisted proof for many years etc.

Example: Given the number 1271, find it's prime factorization.

Instructor's Comments: The answer is 31 times 41. The point here is that even for small numbers humans struggle with this. For not-very-large numbers, even computers struggle.

Factoring a number is a difficult problem and helps form the basis for RSA. If we could factor numbers easily, the RSA encryption we will talk about in the next lecture would be hard.

Instructor's Comments: This next question is completely optional as well. It doesn't add much to RSA. Question: Given $2^n \equiv 9 \pmod{11}$, find n.

Solution: The answer is $n = 6$. However this isn't the real point of this question. The point is that to find 6, you likely tried all the possibilities from

1 to 6 reducing reach time. This problem in general, that is, given a, b and $a^n \in \mathbb{N}$ for some $n \in \mathbb{N}$ to determine n is called the Discrete Logarithm Problem. There is currently no known efficient algorithm to solve it. Solving this would also help break the RSA encryption scheme.

Instructor's Comments: This is probably the 50 minute mark but if not, have fun with the square and multiply algorithm below. This topic is completely optional (as of W2016)

Square and Multiply Algorithm

The idea of this algorithm is to enable computers to compute large powers of integers modulo a natural number n quickly.

Example: Compute $5^{99} \pmod{101}$

Solution: First, we compute successive square powers of 5:

$$\begin{aligned}
5^1 &\equiv 5 \pmod{101} \\
5^2 &\equiv 25 \pmod{101} \\
5^4 &\equiv (25)^2 \equiv 625 \equiv 19 \pmod{101} \\
5^8 &\equiv (19)^2 \equiv 361 \equiv 58 \pmod{101} \\
5^{16} &\equiv (58)^2 \equiv 31 \pmod{101} \\
5^{32} &\equiv (31)^2 \equiv 52 \pmod{101} \\
5^{64} &\equiv (52)^2 \equiv 78 \pmod{101}
\end{aligned}$$

Now, write 99 in binary, that is, as a simple sum of powers of 2 with no power of 2 repeated.

$$\begin{aligned}
64 \leq 99 < 128 \quad &\text{Replace 99 with } 99 - 64 = 35 \\
32 \leq 35 < 64 \quad &\text{Replace 35 with } 35 - 32 = 3 \\
2 \leq 3 < 4 \quad &\text{Replace 3 with } 3 - 2 = 1 \\
1 \leq 1 < 2 \quad &\text{Replace 1 with } 1 - 1 = 0
\end{aligned}$$

Thus, $99 = 64 + 32 + 2 + 1 = 2^6 + 2^5 + 2^1 + 2^0$. Hence,

$$\begin{aligned}
5^{99} &\equiv 5^{64} \cdot 5^{32} \cdot 5^2 \cdot 5^1 \pmod{11} \\
&\equiv 78 \cdot 52 \cdot 25 \cdot 5 \pmod{11} \\
&\equiv 81 \pmod{11}
\end{aligned}$$

Instructor's Comments: Note the minimal number of computations needed. In general, it would be 98 computations. Here it's 6 + 3 =9 computations. A huge savings.

Handout or Document Camera or Class Exercise

(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 $0 \leq x \leq 130$.

Solution:

(i) By Fermat's Little Theorem (valid since $\gcd(2, 131) = 1$,

$$2(2^{129}) \equiv 2^{130} \equiv 1 \pmod{131}$$

(ii) First, we create a chart of the powers of 2:

$$\begin{aligned}
2^1 &\equiv 2 \pmod{131} \\
2^2 &\equiv 4 \pmod{131} \\
2^4 &\equiv 16 \pmod{131} \\
2^8 &\equiv 256 \equiv -6 \pmod{131} \\
2^{16} &\equiv (-6)^2 \equiv 36 \pmod{131} \\
2^{32} &\equiv (36)^2 \equiv 1296 \equiv -14 \pmod{131} \\
2^{64} &\equiv (-14)^2 \equiv 196 \equiv 65 \pmod{131} \\
2^{128} &\equiv (65)^2 \equiv 5^2 \cdot 13^2 \equiv 25 \cdot 169 \equiv 25 \cdot 38 \\
&\equiv 5 \cdot 190 \equiv 5 \cdot 59 \equiv 295 \equiv 33 \pmod{131}
\end{aligned}$$

Hence, $2^{129} \equiv 2^{128} \cdot 2^1 \equiv 33 \cdot 2 \equiv 66 \pmod{131}$.

(iii) Since $2 \cdot 66 \equiv 132 \equiv 1 \pmod{131}$, we see that $2 \cdot (66 \cdot 3) \equiv 3 \pmod{131}$ and since $66 \cdot 3 \equiv 198 \equiv 67 \pmod{131}$, we have completed the question. ■

Lecture 33

Instructor's Comments: I like to introduce Exponentiation Ciphers first and then tackle RSA - this way students can see the build up and see why one prime is an insecure procedure whereas two primes gives a secure procedure.

Exponentiation Cipher

We begin describing RSA by first explaining exponentiation ciphers. Suppose Alice and Bob want to share a message but there is an eavesdropper (Eve) watching their communications.

Instructor's Comments: Include picture while lecturing.

In an exponentiation cipher, Alice chooses a (large) prime p and an e satisfying

$$1 < e < (p-1) \qquad \text{and} \qquad \gcd(e, p-1) = 1.$$

Alice then makes the pair (e, p) public and computes her private key d satisfying

$$1 < d < (p-1) \qquad \text{and} \qquad ed \equiv 1 \pmod{p-1}$$

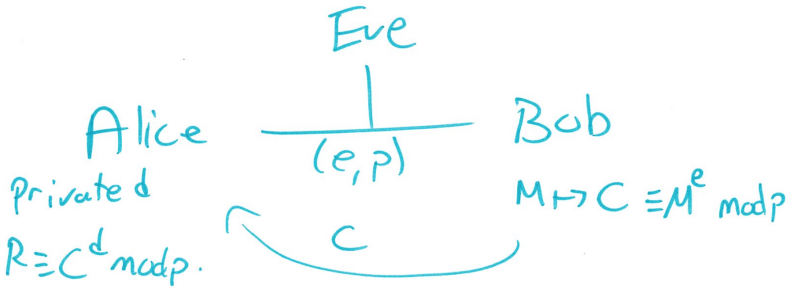
which can be done quickly using the Euclidean Algorithm (the inverse condition above is why we required that $\gcd(e, p-1)$).

To send a message M to Alice, an integer between 0 and $p-1$ inclusive, Bob computes a ciphertext (encrypted message) C satisfying

$$0 \leq C < p \qquad \text{and} \qquad C \equiv M^e \pmod{p}.$$

Bob then sends C to Alice.

Alice then computes $R \equiv C^d \pmod{p}$ with $0 \leq R < p$.



Instructor's Comments: Include picture - this is the 10 minute mark

Proposition: $R \equiv M \pmod{p}$.

Proof: If $p \mid M$, then all of M, C and R are 0 and the claim follows. So we assume that $p \nmid M$. Recall that $ed \equiv 1 \pmod{p-1}$ and so we have that there exists an integer k such that $ed = 1 + k(p-1)$. Using this, we have

$$\begin{aligned} R &\equiv C^d \pmod{p} \\ &\equiv (M^e)^d \pmod{p} && \text{by definition of } C \\ &\equiv M^{ed} \pmod{p} \\ &\equiv M \pmod{p} && \text{Corollary to F}\ell\text{T since } ed \equiv 1 \pmod{p-1}. \end{aligned}$$

as required ■

Corollary: $R = M$

Proof: By the previous proposition, $R \equiv M \pmod{p}$. Recall that $0 \leq M, R < p$ and so the values must be equal. ■

Instructor's Comments: This is the 20 minute mark.

The good news is that this scheme works. However, Eve can compute d just as easily as Alice! Eve knows p, hence knows $p-1$ and can use the Euclidean algorithm to compute d just like Alice. This means our scheme is not secure. To rectify this problem, we include information about two primes.

RSA Alice chooses two (large) distinct primes p and q, computes $n = pq$ and selects any e satisfying

$$1 < e < (p-1)(q-1) \qquad \text{and} \qquad \gcd(e, (p-1)(q-1)) = 1$$

Alice then makes the pair (e, n) public and compute her private key d satisfying

$$1 < d < (p-1)(q-1) \qquad \text{and} \qquad ed \equiv 1 \pmod{(p-1)(q-1)}$$

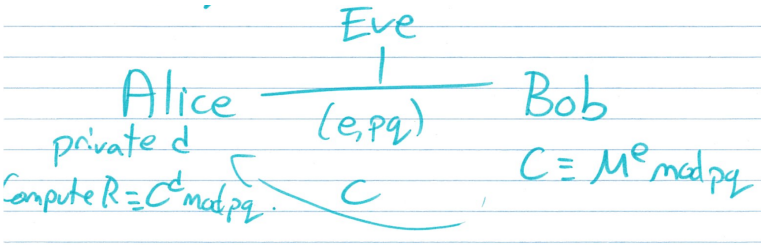
again which can be done quickly using the Euclidean Algorithm (Alice knows p and q and hence knows $(p-1)(q-1)$).

Instructor's Comments: Note that in the textbook (d, n) is the private key pair.

To send a message M to Alice, an integer between 0 and $n-1$ inclusive, Bob computes a ciphertext C satisfying

$$0 \leq C < pq \qquad \text{and} \qquad C \equiv M^e \pmod{pq}.$$

Bob then sends C to Alice. Alice then computes $R \equiv C^d \pmod{pq}$ with $0 \leq R < pq$.



Instructor's Comments: Include a diagram of what's happening. This is the 30 minute mark.

Proposition: $R = M$.

Proof: Since $ed \equiv 1 \pmod{(p-1)(q-1)}$, transitivity of divisibility tells us that

$$ed \equiv 1 \pmod{p-1} \qquad \text{and} \qquad ed \equiv 1 \pmod{q-1}.$$

Since $\gcd(e, (p-1)(q-1)) = 1$, GCD Prime Factorization (or by definition) tells us that $\gcd(e, p-1) = 1$ and that $\gcd(e, q-1) = 1$. Next, as $C \equiv M^e \pmod{pq}$, Splitting the Modulus states that

$$C \equiv M^e \pmod{p} \qquad \text{and} \qquad C \equiv M^e \pmod{q}$$

Similarly, by Splitting the Modulus, we have

$$R \equiv C^d \pmod{p} \qquad \text{and} \qquad R \equiv C^d \pmod{q}.$$

By the previous proposition applied twice, we have that

$$R \equiv M \pmod{p} \qquad \text{and} \qquad R \equiv M \pmod{q}.$$

Now, an application of the Chinese Remainder Theorem (or Splitting the Modulus), valid since p and q are distinct, gives us that $R \equiv M \pmod{pq}$. Recalling that $0 \leq R, M < pq$, we see that $R = M$. ■

Is this scheme more secure? Can Eve compute d? If Eve can compute $(p-1)(q-1)$ then Eve could break RSA. To compute this value given only n (which recall is pq), Eve would need to factor n (or compute $p+q$). Factoring n is a notoriously hard problem and we know of no quick way of doing so. Eve could also break RSA if she could solve the problem of computing M given $M^e \pmod{n}$.

Note: Let ϕ be the Euler Phi Function. This function has the valuation $\phi(n) = (p-1)(q-1)$ when $n = pq$ a product of distinct primes.

Instructor's Comments: This is the 40 minute mark

Handout or Document Camera or Class Exercise

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).

Solution:

(i) Note $n = 22$, $\phi(n) = (2-1)(11-1) = 10$ and lastly, $3d \equiv 1 \pmod{10}$ and multiplying by 7 gives $d \equiv 7 \pmod{10}$. Hence $d = 7$.

(ii) Note that

$$\begin{aligned} C &\equiv M^e \pmod{22} \\ &\equiv 8^3 \pmod{22} \\ &\equiv 8 \cdot 64 \pmod{22} \\ &\equiv 8 \cdot (-2) \pmod{22} \\ &\equiv -16 \pmod{22} \\ &\equiv 6 \pmod{22} \end{aligned}$$

(iii) The quick way to solve this is to recall the RSA theorem and hence $M = 8$. The long way is to do the following:

$$\begin{aligned} R &\equiv C^d \pmod{22} \\ &\equiv 6^7 \pmod{22} \\ &\equiv 6 \cdot (6^3)^2 \pmod{22} \\ &\equiv 6 \cdot (216)^2 \pmod{22} \\ &\equiv 6 \cdot (-4)^2 \pmod{22} \\ &\equiv 6 \cdot 16 \pmod{22} \\ &\equiv 6 \cdot (-6) \pmod{22} \\ &\equiv -36 \pmod{22} \\ &\equiv 8 \pmod{22} \end{aligned}$$

Food for thought:

(i) How does Alice choose primes p and q? (Answer: Randomly choose odd numbers! If p and q are 100 digit primes, then choosing 100 gives you more than a 50% chance that you have a prime - can check using primality tests).

(ii) What if Eve wasn't just a passive eavesdropper? What if Eve could change the public key information before it reaches Bob? (This involves using certificates).

(iii) What are some advantages of RSA? (Believed to be secure, uses the same hardware for encryption and decryption, computations can be done quickly using a square and multiply algorithm).

Lecture 34

Instructor's Comments: There's a large probability that you might have extra time in this lecture - there are ways to fill that time in later lectures with some extra complex numbers proofs.

Complex Numbers

Our current view of important sets:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

These sets can be thought of as helping us to solve polynomial equations. However, $x^2 + 1 = 0$ has no solution in any of these sets.

Instructor's Comments: This is the 3 minute mark

Definition: A complex numbers (in standard form) is an expression of the form $x + yi$ where $x, y \in \mathbb{R}$ and i is the imaginary unit. Denote the set of complex numbers by

$$\mathbb{C} := \{x + yi : x, y \in \mathbb{R}\}$$

Example: $1 + 2i$, $3i$, $\sqrt{13} + \pi i$, 2 (or $2 + 0i$).

Note:

(i) $\mathbb{R} \subseteq \mathbb{C}$

(ii) If $z = x + yi$, then $x = \text{Re}(z) = \Re(z)$ is called the real part and $y = \text{Im}(z) = \Im(z)$ is called the imaginary part.

Definition: Two complex numbers $z = x + yi$ and $w = u + vi$ are equal if and only if $x = u$ and $y = v$.

Definition: A complex number $z = x + yi$ is...

(i) Purely real (or simply real) if $\Im(z) = 0$, that is, $z = x$

(ii) Purely Imaginary if $\Re(z) = 0$, that is, $x = yi$.

We turn $\mathbb{C}$ into a commutative ring by defining operations as follows:

(i) $(x + yi) \pm (u + vi) := (x \pm u) + (y \pm v)i$

(ii) $(x + yi)(u + vi) := (xu - vy) + (xv + uy)i$

By this definition, we have

$$i^2 = i \cdot i = (0 + i)(0 + i) = -1 + 0i = -1.$$

Therefore, i is a solution of $x^2 + 1$. With this in mind, you can remember multiplication just by multiplying terms as you would with polynomials before.

$$(x + yi)(u + vi) = xu + xvi + yiu + yivi = xu + (xv + yu)i + yvi^2 = xu - yv + (xv + uy)i$$

Example:

(i) $(1+2i)+(3+4i)=4+6i$

(ii) $(1+2i)-(3+4i)=-2-2i$

(iii) $(1+2i)(3+4i)=3-8+(4+6)i=-5+10i$

We note that $\mathbb{C}$ is a field by observing that the multiplicative inverse of a nonzero complex numbers is

$$(x+yi)^{-1}=\frac{x}{x^2+y^2}-\frac{y}{x^2+y^2}i$$

Exercise: If $z\in\mathbb{C}$ and $z\neq 0$, then $z\cdot z^{-1}=1$

Instructor's Comments: This is the 20-25 minute mark.

For complex numbers u,v,w,z with v and z nonzero, the above is consistent with the usual fraction rules:

$$\frac{u}{v}+\frac{w}{z}=\frac{uz+vw}{vz} \qquad \text{and} \qquad \frac{u}{v}\cdot\frac{w}{z}=\frac{uw}{vz}$$

For $k\in\mathbb{N}$ and $z\in\mathbb{C}$, define

$$z^0=1 \qquad z^1=z \qquad z^{k+1}=z\cdot z^k$$

and further that $z^{-k}:=(z^{-1})^k$. With these definitions, the usual exponent rules hold, namely

$$z^{m+n}=z^m\cdot z^n \qquad (z^m)^n=z^{mn}$$

for $m,n\in\mathbb{Z}$.

Example: Write $\frac{1+2i}{3-4i}$ in standard form.

Solution:

$$\begin{aligned}
\frac{1+2i}{3-4i} &= (1+2i)(3-4i)^{-1} \\
&= (1+2i)\left(\frac{3}{3^2+4^2}-\frac{(-4)}{3^2+4^2}i\right) \\
&= (1+2i)\left(\frac{3}{25}+\frac{4}{25}i\right) \\
&= \frac{3}{25}-\frac{8}{25}+\left(\frac{4}{25}+\frac{6}{25}\right)i \\
&= \frac{-5}{25}+\frac{10}{25}i \\
&= \frac{-1}{5}+\frac{2}{5}i
\end{aligned}$$

Instructor's Comments: This is the 30 minute mark

Handout or Document Camera or Class Exercise

Express the following in standard form

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

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

Solution:

(i)

$$\begin{aligned} z &= ((1-2i)-(3+4i))(5-6i)^{-1} \\ &= (-2-6i)\left(\frac{5}{5^2+6^2} - \frac{(-6)}{5^2+6^2}i\right) \\ &= (-2-6i)\left(\frac{5}{61} + \frac{6}{61}i\right) \\ &= \frac{-10}{61} + \frac{36}{61} + \left(\frac{-12}{61} - \frac{30}{61}\right)i \\ &= \frac{26}{61} - \frac{42}{61}i \end{aligned}$$

(ii) Recall that $i^2 = -1$ and $i^4 = 1$. Thus,

$$\begin{aligned} w &= i^{2015} \\ &= (i^4)^{503} \cdot i^3 \\ &= 1^{503} \cdot i^2 \cdot i \\ &= -i \end{aligned}$$

Instructor's Comments: This is the 40 minute mark - you can easily go on to the next lecture or use this time to catch up.

Lecture 35

Instructor's Comments: The following is a technical note. In the textbook, they use the quadratic formula without any real justification as to why it makes sense with the rest of complex numbers. Here I justify it over real polynomials (and then later we'll make a note that it holds over complex polynomials)

Instructor's Comments: This is a great spot to catch up if you're behind. I would advise grouping the four 'work on their own' problems together at the end of class and spend the last say 15-20 minutes battling through them. Then get students to ask to take one of them up. If doing this I suggest starting with the last problem then mentions the first two in this lecture. The last problem is very easy and they shouldn't have problems. The first two are challenging and you want them to battle through it a bit more. Whatever you get done in class great. Tell them to do the others for homework and refer them to the online notes if they can't solve them.

Example: For $z \in \mathbb{C}$, solve $z^2 - z + 1 = 0$.

Instructor's Comments: Note to students that z will almost exclusively stand for a complex number in this course.

Solution: Ideally, we'd like to write something like

$$z = \frac{-(-1) \pm \sqrt{(-1)^2 - 4(1)(1)}}{2(1)} = \frac{1 \pm \sqrt{-3}}{2} = \frac{1 \pm \sqrt{3}i}{2}.$$

However there is one big gap. The expression $\sqrt{-3}$ has no meaning. Not to mention, we have not discussed what the solutions are to $\sqrt{-3}$ as a complex number. Are there 2 solutions? One solution? Ten solutions? Zero solutions? This needs to be addressed.

Question: What are the solutions to $z^2 = -r$ for $r \in \mathbb{R}$ with $r > 0$?

Solution: Let $z = x + yi$ with $x, y \in \mathbb{R}$. Then

$$-r = z^2 = (x + yi)^2 = x^2 - y^2 + 2xyi$$

Therefore, $2xy = 0$ and $x^2 - y^2 = -r$. Thus, either $x = 0$ or $y = 0$. If $y = 0$, then $x^2 = -r$, a contradiction since $x^2 \geq 0$. Hence, $x = 0$ and $-y^2 = -r$ or $y = \pm\sqrt{r}$. Therefore, $z = \pm\sqrt{r}i$. ■

Note: Therefore, we have just validated the use of $\sqrt{-r} = \pm\sqrt{r}i$. The quadratic formula still works for real polynomials (and later we will see it still works for complex polynomials).

Proposition: If the discriminant Δ of a real polynomial $az^2 + bz + c$ is negative, zeroes of the equation are given by

$$z = \frac{-b \pm \sqrt{-\Delta}i}{2a}$$

Solution: We complete the square as usual:

$$\begin{aligned} a\left(z^2+\frac{b}{a}z\right)+c&=0\\ a\left(z^2+\frac{b}{a}z+\left(\frac{b}{2a}\right)^2-\left(\frac{b}{2a}\right)^2\right)+c&=0\\ a\left(z^2+\frac{b}{a}z+\left(\frac{b}{2a}\right)^2\right)-\left(\frac{b^2}{4a}\right)+c&=0\\ a\left(z+\frac{b}{2a}\right)^2&=\left(\frac{b^2}{4a}\right)-c \end{aligned}$$

Clearing denominators and moving the outer factor in the square term gives

$$(2az+b)^2=b^2-4ac=\Delta$$

Now, since $\Delta<0$, we can apply the previous result to get that the solutions to this equation are given by

$$\begin{aligned} 2az+b&=\pm\sqrt{-\Delta}i\\ 2az&=-b\pm\sqrt{-\Delta}i\\ z&=\frac{-b\pm\sqrt{-\Delta}i}{2a} \end{aligned}$$

as stated in the claim. ■

The above essentially states that the quadratic formula works as usual if we believe a common convention that $\sqrt{-\Delta}$ is equal to $\sqrt{\Delta}i$ (We shouldn't be writing square roots of negative numbers however!)

Definition: The complex conjugate of a complex number $z=x+yi$ is $\overline{z}:=x-yi$.

Instructor's Comments: This is the 13 minute mark

Handout or Document Camera or Class Exercise

Instructor's Comments: Give the next two exercises simultaneously for students to battle through

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

Solution: Let $z = x + yi$ where $x, y \in \mathbb{R}$. Then

$$\begin{aligned} (x+yi)^2 &= i(x-yi) \\ x^2 - y^2 + 2xyi &= y + xi \\ x^2 - y^2 = y \qquad &\text{and} \qquad 2xy = x \end{aligned}$$

The latter implies that $2xy - x = 0$ and hence $x(2y-1) = 0$. Therefore, either $x = 0$ or $y = \frac{1}{2}$. Substituting into the first equation above gives

$$\begin{aligned} x = 0 &\implies -y^2 = y \implies y^2 + y = 0 \implies y = 0 \text{ or } -1 \\ y = \tfrac{1}{2} &\implies x^2 - (\tfrac{1}{2})^2 = \tfrac{1}{2} \implies x^2 = \tfrac{3}{4} \implies x = \pm\tfrac{\sqrt{3}}{2} \end{aligned}$$

Hence, $z \in \{0, -i, \frac{\sqrt{3}}{2} + \frac{1}{2}i, \frac{-\sqrt{3}}{2} + \frac{1}{2}i\}$. ■

Handout or Document Camera or Class Exercise

Find a real solution to

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

Solution: Take $z = r \in \mathbb{R}$. Then, if this r is a solution, it must satisfy

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

Expanding and collecting terms gives

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

Therefore, $3\sqrt{2}r^2 + 2\sqrt{2}r = 0$. Factoring gives $\sqrt{2}r(3r+2) = 0$ and thus, $r = 0$ or $r = \frac{-2}{3}$. Since the real part above must also be zero, we see that the r must satisfy

$$6r^3 + r^2 - 11r - 6 = 0$$

Note that $r = 0$ is not a solution to this and that $r = \frac{-2}{3}$ is a solution since

$$6(\tfrac{-2}{3})^3 + (\tfrac{-2}{3})^2 - 11 \cdot \tfrac{-2}{3} - 6 = 6 \cdot \tfrac{-8}{27} + \tfrac{4}{9} + \tfrac{22}{3} - 6 = 0$$

Thus, $r = \frac{-2}{3}$ is the lone solution. ■

Instructor's Comments: This is the 35 minute mark

Proposition: (Properties of Conjugates (PCJ)) Let $z, w \in \mathbb{C}$. Then

(i) $\overline{z+w} = \overline{z} + \overline{w}$

(ii) $\overline{zw} = \overline{z} \cdot \overline{w}$

(iii) $\overline{\overline{z}} = z$

(iv) $z + \overline{z} = 2\Re(z)$

(v) $z - \overline{z} = 2i\Im(z)$.

Instructor's Comments: For your sanity's sake, you should only do a few of these, say 2 and 3.

Solution: Let $z = x + yi$ and $w = u + vi$. Then

(i)

$$\begin{aligned}
\overline{z+w} &= \overline{x + yi + u + vi} \\
&= \overline{(x+u) + (y+v)i} \\
&= (x+u) - (y+v)i \\
&= x - yi + u - vi \\
&= \overline{z} + \overline{w}
\end{aligned}$$

(ii)

$$\begin{aligned}
\overline{zw} &= \overline{(x+yi)(u+vi)} \\
&= \overline{(xu - yv) + (xv + uy)i} \\
&= (xu - yv) - (xv + uy)i \\
&= (x - yi)(u - vi) \\
&= \overline{zw}
\end{aligned}$$

(iii) $\overline{\overline{z}} = \overline{\overline{x + yi}} = \overline{x - yi} = x + yi = z$

(iv) $z + \overline{z} = x + yi + x - yi = 2x = 2\Re(z)$

(v) $z - \overline{z} = x + yi - (x - yi) = 2yi = 2i\Im(z)$

Instructor's Comments: This is the 40 minute mark.

Handout or Document Camera or Class Exercise

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 $z = -\bar{z}$.

Instructor's Comments: Note that 0 is both real and purely imaginary.

Solution:

(i) ($\Rightarrow$) Let $z = x + 0i \in \mathbb{R}$. Then $\overline{z} = x - 0i = x = z$.

($\Leftarrow$) Let $z = x + yi$ for $x, y \in \mathbb{R}$. Assume that $z = \overline{z}$. Then,

$$\begin{aligned} z &= \overline{z} \\ x + yi &= x - yi \\ y &= -y \\ 2y &= 0 \\ y &= 0 \end{aligned}$$

Therefore, $z = x + 0i \in \mathbb{R}$. ■

(ii)

$$\begin{aligned} z \text{ is purely imaginary} &\Leftrightarrow iz \in \mathbb{R} \\ &\Leftrightarrow iz = \overline{iz} && \text{By the above} \\ &\Leftrightarrow iz = -i\overline{z} && \text{By PCJ} \\ &\Leftrightarrow z = -\overline{z} \end{aligned}$$

completing the proof. ■

Instructor's Comments: This is the 50 minute mark.

Lecture 36

Handout or Document Camera or Class Exercise

Instructor's Comments: There are two clicker questions here. Choose the one you prefer. I like the first one because students often forget they can use LDEs to find inverses.

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

Solution: We use the Extended Euclidean Algorithm (EEA) on $241x + 1001y = 1$ to see that

x	y	r	q
0	1	1001	0
1	0	241	0
-4	1	37	$\lfloor \frac{1001}{241} \rfloor = 4$
25	-6	19	$\lfloor \frac{241}{37} \rfloor = 6$
-29	7	18	$\lfloor \frac{37}{19} \rfloor = 1$
54	-13	1	$\lfloor \frac{19}{18} \rfloor = 1$

Hence $241(54) + 1001(-13) = 1$ and so $[54]$ is the inverse of $[241]$ in $\mathbb{Z}_{1001}$. Since $5 + 4 = 9$, the correct answer is B.

Handout or Document Camera or Class Exercise

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

$$\begin{aligned} x &\equiv 6 \pmod{13} \\ 4x &\equiv 3 \pmod{7} \\ -1000 &< x < 1000 \end{aligned}$$

A) 1

B) 7

C) 13

D) 22

E) 91

Solution: Note that multiplying $4x \equiv 3 \pmod 7$ by 2 gives $x \equiv 6 \pmod 7$. By the Chinese Remainder Theorem or by Splitting the Modulus, we see that $x \equiv 6 \pmod{91}$. Thus, $x = 6 + 91k$. Using this with the range restriction gives

$$\begin{aligned} -1000 &< 6 + 91k < 1000 \\ -1006 &< 91k < 994 \end{aligned}$$

Note that $91 \cdot 10 = 910$ and $91 \cdot 11 = 1001$. Therefore, the above condition with the fact that $k \in \mathbb{Z}$ reduces to $-11 \leq k \leq 10$ and thus, there are 22 solutions.

Instructor's Comments: This is the 10 minute mark; this is a longer problem

Definition: The modulus of $z = x + yi$ is the nonnegative real number

$$|z| = |x + yi| := \sqrt{x^2 + y^2}$$

Proposition: (Properties of Modulus (PM))

(i) $|\overline{z}| = |z|$

(ii) $z\overline{z} = |z|^2$

(iii) $|z| = 0 \Leftrightarrow z = 0$

(iv) $|zw| = |z||w|$

(v) $|z + w| \leq |z| + |w|$ (This is called the triangle inequality)

Instructor's Comments: Mention that properties 3,4,5 define a norm. I recommend not doing the proof of all of these. I would do 2,4 and 5. In fact, I would make 5 an in-class reading proof to get some reading practice in.

Proof: Throughout, let $z = x + yi$.

(i) Note that

$$|\overline{z}| = |x - yi| = \sqrt{x^2 + (-y)^2} = \sqrt{x^2 + y^2} = |z|$$

(ii) $z\overline{z} = (x + yi)(x - yi) = x^2 + y^2 = |z|^2$

(iii) $|z| = 0$ if and only if $\sqrt{x^2 + y^2} = 0$ if and only if $x^2 + y^2 = 0$ if and only if $x = y = 0$ if and only if $z = 0$.

(iv) Using the second property above and Properties of Conjugates, we have

$$|zw|^2 = (zw)\overline{zw} = z\overline{z}w\overline{w} = |z|^2|w|^2$$

Hence, since all the numbers above are real, we have that $|zw| = |z||w|$.

(v) (See the handout on next page)

Handout or Document Camera or Class Exercise

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

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

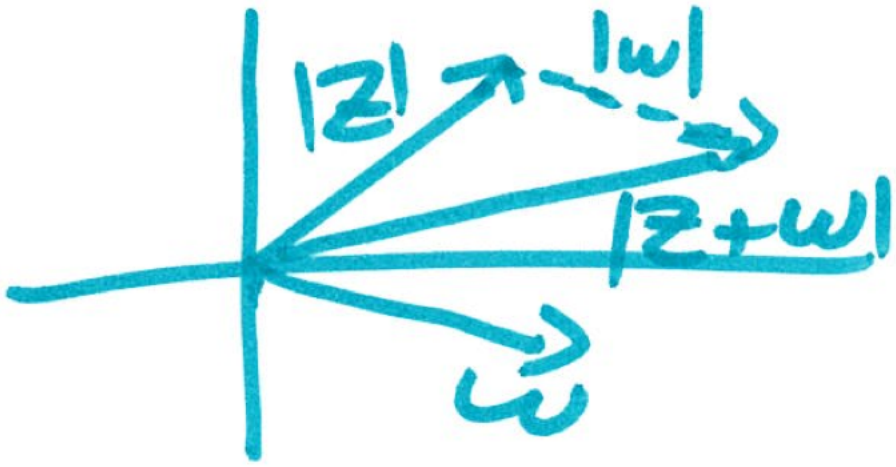
Now, from Properties of Conjugates, we have that

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

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.



Instructor's Comments: This is the 25-30 minute mark

Revisit Inverses

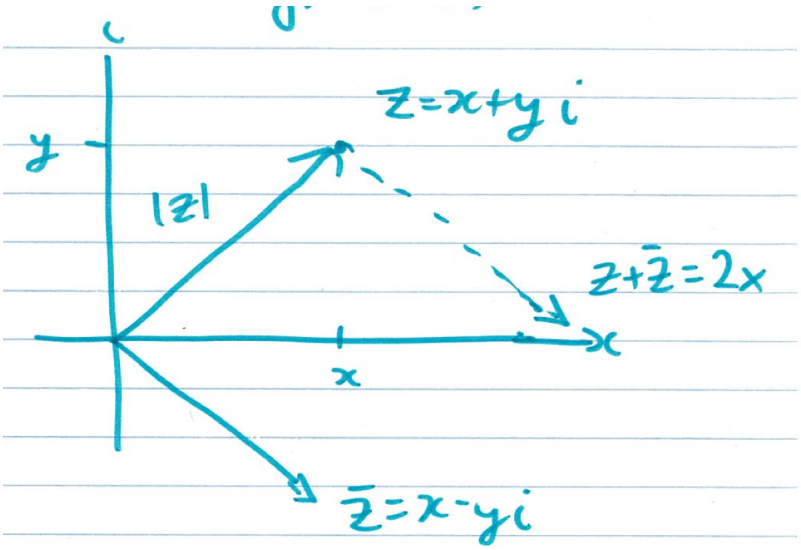
Recall, we defined the inverse of z by

$$z^{-1} = \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}i$$

Note that

$$z^{-1} = \frac{1}{z}\cdot\frac{\overline{z}}{\overline{z}} = \frac{\overline{z}}{z\cdot\overline{z}} = \frac{\overline{z}}{|z|^2}$$

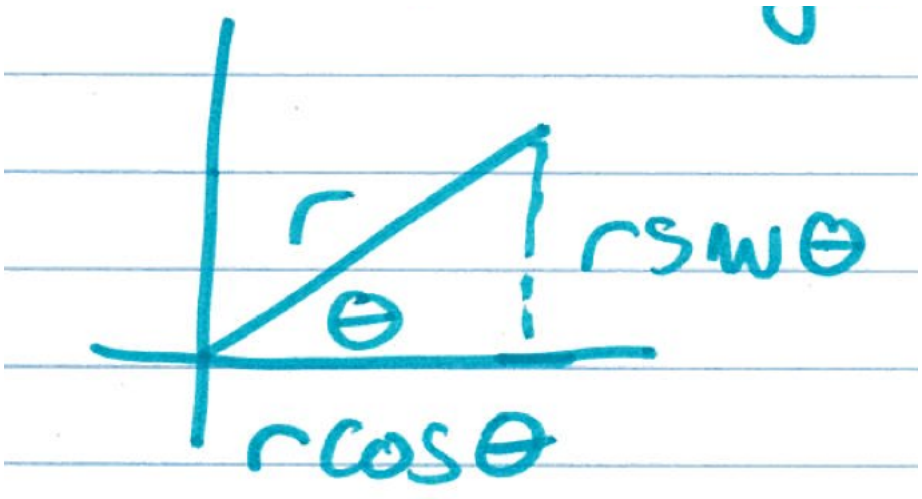
Argand Diagram



Instructor's Comments: This is the 35 minute mark.

Polar Coordinates

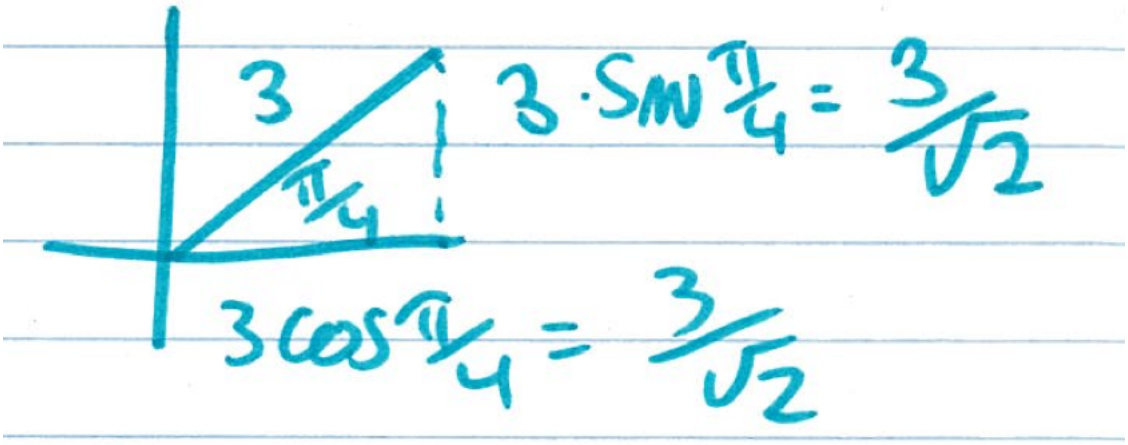
A point in the plane corresponds to a length and an angle:



Example: $(r,\theta) = (3, \frac{\pi}{4})$ corresponds to

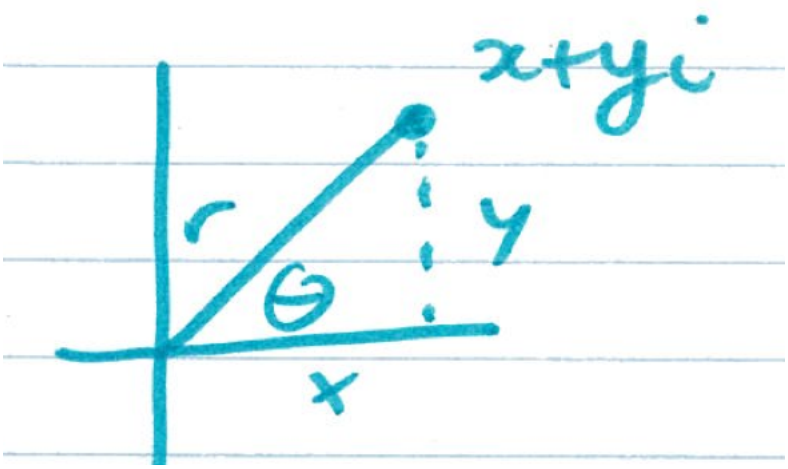
$$3\cos(\pi/4) + i(3\sin(\pi/4)) = \frac{3}{\sqrt{2}} + \frac{3}{\sqrt{2}}i$$

via the picture



Given $z = x + yi$, we see that

$$r = |z| = \sqrt{x^2 + y^2}$$
$$\theta = \arccos(x/r) = \arcsin(y/r) = \arctan(y/x)$$



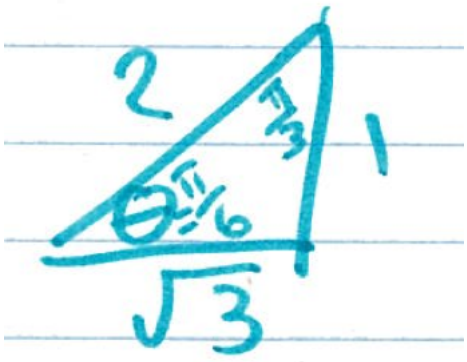
Note: WARNING. The angle θ might be $\arctan(y/x)$ OR $\pi + \arctan(y/x)$ depending on which quadrant we are in. More on this next class.

Example: Write $z = \sqrt{6} + \sqrt{2}i$ using polar coordinates.

Solution: Note that $r = \sqrt{\sqrt{6}^2 + \sqrt{2}^2} = \sqrt{8} = 2\sqrt{2}$. Further,

$$\arctan(\sqrt{2}/\sqrt{6}) = \arctan 1/\sqrt{3} = \pi/6$$

Note: There is no need to add π to the above answer since the answer lies in the first quadrant.



Therefore, z corresponds to $(r, \theta) = (2\sqrt{2}, \pi/6)$. ■

Definition: The polar form of a complex number z is $z = r(\cos(\theta) + i\sin(\theta))$ where r is the modulus of z and θ is called *an* argument of z. This is sometimes denoted by $\arg(z) = \theta$. Further, denote $\text{cis}(\theta) := \cos(\theta) + i\sin(\theta)$.

Example: If $z = \sqrt{6} + \sqrt{2}i$, then $z = 2\sqrt{2}(\cos(\pi/6) + i\sin(\pi/6)) = 2\sqrt{2}\text{cis}(\pi/6)$.

Instructor's Comments: This is the 50 minute mark.

Lecture 37

Handout or Document Camera or Class Exercise

Express the following in terms of polar coordinates:

(i) -3

(ii) $1-i$

Solution:

(i) Note that $r = |-3| = 3$ and $\theta = \arctan(0/-3) = 0$. Then, since -3 lives between the second and third quadrant, you need to add π to the previous answer. Thus $\theta = \pi$ and hence $-3 = 3\text{cis}(\pi)$.

Instructor's Comments: Make sure to note the addition of pi above.

(ii) Note that $r = |1-i| = \sqrt{1^2+1^2} = \sqrt{2}$. Hence

$$\begin{aligned} 1-i &= \sqrt{2}\left(\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}\right) \\ &= \sqrt{2}(\cos(7\pi/4) + i\sin(7\pi/4)) \\ &= \sqrt{2}\text{cis}(7\pi/4) \end{aligned}$$

Instructor's Comments: This is the 10 minute mark.

Handout or Document Camera or Class Exercise

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

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

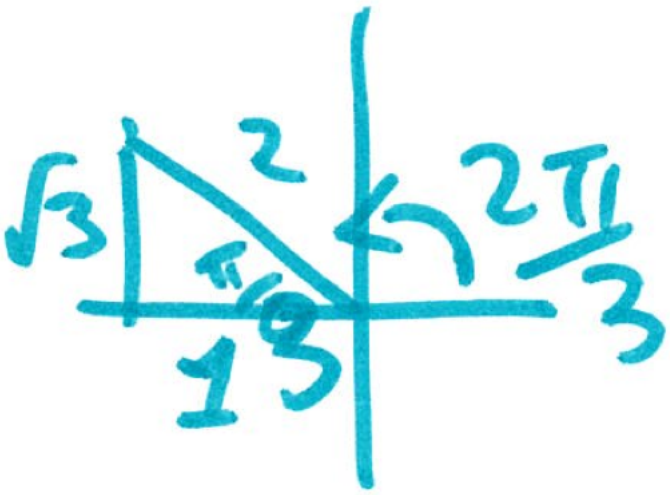
Solution:

(i) $\text{cis}(15\pi/6) = \cos(5\pi/2) + i\sin(5\pi/2) = i$.

(ii) Note that

$$\begin{aligned} r &= |-3\sqrt{2}+3\sqrt{6}i| \\ &= \sqrt{(-3\sqrt{2})^2+(3\sqrt{6})^2} \\ &= \sqrt{18+54} \\ &= \sqrt{72} \\ &= 6\sqrt{2} \end{aligned}$$

Therefore, $-3\sqrt{2}+3\sqrt{6}i = 6\sqrt{2}\left(\frac{-1}{2}+\frac{\sqrt{3}}{2}i\right) = 6\sqrt{2}\text{cis}(2\pi/3)$ where the last equality holds since



Instructor's Comments: This is the 20 minute mark

Theorem: (Polar Multiplication of Complex Numbers (PMCN)) If $z_1 = r_1\text{cis}(\theta_1)$ and $z_2 = r_2\text{cis}(\theta_2)$, then

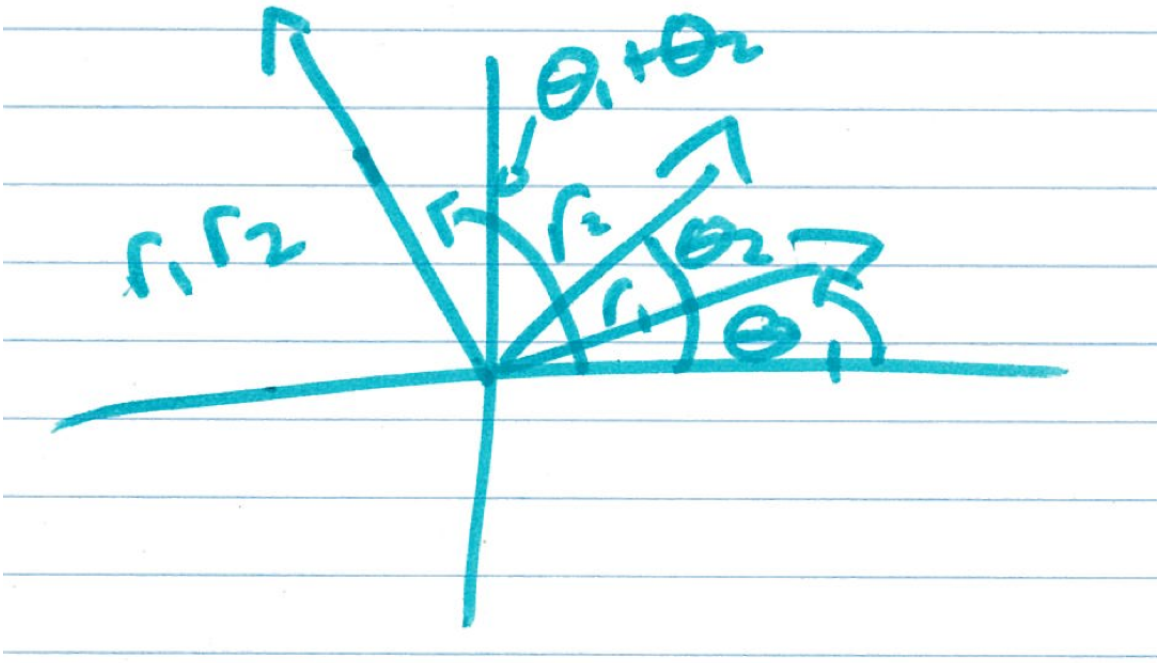
$$z_1 z_2 = r_1 r_2 \text{cis}(\theta_1 + \theta_2)$$

Proof: We have

$$\begin{aligned} z_1 z_2 &= r_1(\cos(\theta_1) + i\sin(\theta_1))r_2(\cos(\theta_2) + i\sin(\theta_2)) \\ &= r_1 r_2(\cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2) + i(\cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2))) \\ &= r_1 r_2(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)) \\ &= r_1 r_2 \text{cis}(\theta_1 + \theta_2) \end{aligned}$$

where in line 3 above, we used trig identities. This completes the proof. ■

Corollary: Multiplication by $i = \cos(\pi/2) + i\sin(\pi/2)$ gives a rotation by $\pi/2$.



Example: Using Polar Multiplication of Complex Numbers on $(\sqrt{6}+\sqrt{2}i)(-3\sqrt{2}+3\sqrt{6}i)$ gives

$$\begin{aligned} (\sqrt{6} + \sqrt{2}i)(-3\sqrt{2} + 3\sqrt{6}i) &= 2\sqrt{2}\text{cis}(\pi/6) \cdot 6\sqrt{2}\text{cis}(2\pi/3) \\ &= 24\text{cis}(\pi/6 + 2\pi/3) \qquad \text{By PMCN} \\ &= 24\text{cis}(5\pi/6) \\ &= 24(-\sqrt{3}/2 + i/2) \\ &= -12\sqrt{3} + 12i \end{aligned}$$

Instructor's Comments: This is the 30-35 minute mark.

Theorem: (De Moivre's Theorem (DMT)) If $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$, then

$$(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$$

or more compactly,

$$\text{cis}(\theta)^n = \text{cis}(n\theta).$$

Instructor's Comments: Emphasize here that we want to use induction but need to reduce to the natural numbers first

Proof: First note that when $n = 0$, we see that $(\cos(\theta) + i\sin(\theta))^0 = 1$ and that $\cos(0\theta) + i\sin(0\theta) = 1$ so the statement holds. For $n > 0$, we proceed by induction on n. For the base case, consider $n = 1$. Then

$$(\cos(\theta) + i\sin(\theta))^n = \cos(\theta) + i\sin(\theta) = \cos(n\theta) + i\sin(n\theta).$$

Now, assume that

$$(\cos(\theta) + i\sin(\theta))^k = \cos(k\theta) + i\sin(k\theta)$$

holds for some $k \in \mathbb{N}$. For the inductive step, note that

$$\begin{aligned}
(\cos(\theta) + i\sin(\theta))^{k+1} &= (\cos(\theta) + i\sin(\theta))^k(\cos(\theta) + i\sin(\theta)) \\
&= (\cos(k\theta) + i\sin(k\theta))(\cos(\theta) + i\sin(\theta)) && \text{Inductive hypothesis} \\
&= \cos((k+1)\theta) + i\sin((k+1)\theta) && \text{By PMCN}
\end{aligned}$$

For $n < 0$, we write $n = -m$ for some $m \in \mathbb{N}$. Then

$$\begin{aligned}
\text{cis}(\theta)^n &= \text{cis}(\theta)^{-m} \\
&= (\text{cis}(\theta)^m)^{-1} \\
&= \text{cis}(m\theta)^{-1} \\
&= \frac{\cos(m\theta) - i\sin(m\theta)}{\cos^2(m\theta) + \sin^2(m\theta)} && \text{Since } z^{-1} = \overline{z}/|z|^2 \\
&= \cos(m\theta) - i\sin(m\theta)
\end{aligned}$$

and $\cos(-m\theta) + i\sin(-m\theta) = \cos(m\theta) - i\sin(m\theta)$ since cosine is even and sine is odd. This completes the proof. ■

Corollary: If $z = r\text{cis}(\theta)$ then $z^n = r^n\text{cis}(n\theta)$.

Instructor's Comments: This is the 50 minute mark.

Lecture 38

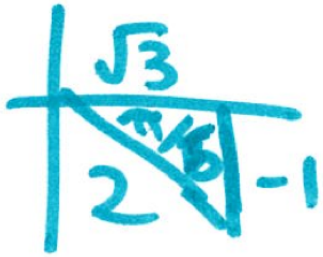
Handout or Document Camera or Class Exercise

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

Solution: Convert $\sqrt{3}-i$ to polar coordinates.

$$\begin{aligned}\sqrt{3}-i &= 2\left(\frac{\sqrt{3}}{2}-\frac{i}{2}\right)\\ &= 2\text{cis}(-\pi/6)\\ &= 2\text{cis}(11\pi/6)\end{aligned}$$

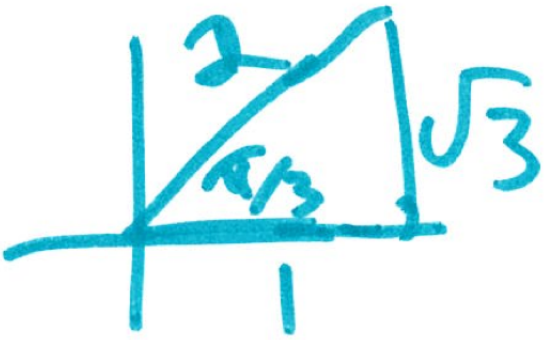
seen via the diagram



Lastly,

$$\begin{aligned}(2\text{cis}(11\pi/6))^{10} &= 2^{10}\text{cis}(110\pi/6) && \text{DMT}\\ &= 2^{10}\text{cis}(55\pi/3)\\ &= 2^{10}\text{cis}(9(2\pi)+\pi/3)\\ &= 2^{10}\text{cis}(\pi/3)\\ &= 2^{10}\left(\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)\\ &= 2^9+2^9\sqrt{3}i\\ &= 512+512\sqrt{3}i\end{aligned}$$

seen via the diagram



Instructor's Comments: This is the 10-15 minute mark

Complex Exponential Function

Definition: For a real θ, define

$$e^{i\theta} := \cos(\theta) + i\sin(\theta) = \text{cis}(\theta)$$

Note: Can write $z \in \mathbb{C}$ as $z = re^{i\theta}$ where $r = |z|$ and θ is an argument of z.

Question: Why is this definition reasonable? While we can't prove the answer to this question, we can give convincing arguments.

Reason 1: Exponential Laws Work! For $\theta, \alpha \in \mathbb{R}$ and $n \in \mathbb{N}$,

$$\begin{aligned} e^{i\theta} \cdot e^{i\alpha} &= e^{i(\theta+\alpha)} && \text{PMCN} \\ (e^{i\theta})^n &= e^{in\theta} && \text{DMT} \end{aligned}$$

Reason 2: Derivative with respect to θ makes sense.

$$\begin{aligned} \frac{d}{d\theta}(\cos(\theta) + i\sin(\theta)) &= -\sin(\theta) + i\cos(\theta) \\ &= i(\cos(\theta) + i\sin(\theta)) \\ &= ie^{i\theta} \end{aligned}$$

Reason 3: Power series.

$$\begin{aligned} e^x &= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots \\ \sin(x) &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \ldots \\ \cos(x) &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \ldots \end{aligned}$$

Using these and combining gives

$$e^{ix} = \cos(x) + i\sin(x)$$

Setting $\theta = \pi$ gives Euler's Formula:

$$e^{i\pi} = \cos(\pi) + i\sin(\pi) = -1$$

Instructor's Comments: This is the 25 minute mark.

Example: Write $(2e^{11\pi/6})^6$ in standard form.

Solution: By exponent rules (DMT), we have

$$\begin{aligned} (2e^{11\pi/6})^6 &= 2^6 e^{11\pi i} \\ &= 2^6(\cos(11\pi) + i\sin(11\pi)) \\ &= 2^6(-1 + 0i) \\ &= -64 \end{aligned}$$

Instructor's Comments: This is the 30 minute mark.

Example: Solve $z^6 + 2z^3 - 3 = 0$

Solution: Factoring gives

$$0 = z^6 + 2z^3 - 3 = (z^3 - 1)(z^3 + 3)$$

Hence $z^3 = 1$ or $z^3 = -3$.

Question: Can we solve $z^n = w$ for a fixed $w \in \mathbb{C}$?

Note: We saw a case of this already with $n = 2$ and $w = -r$. We'll delay the previous question until later.

Example: Solve $z^6 = -64$.

Solution: We already saw that $2e^{11\pi/6}$ was a solution. Note that $\pm 2i$ are two others found by inspection. How do we find all the solutions in general? The answer involves using polar coordinates. Write $z = re^{i\theta}$. Then

$$z^6 = r^6 e^{i6\theta} = -64$$

Taking the modulus yields $|r|^6 |e^{i6\theta}| = 64$. Since for any real α, we have

$$|e^{i\alpha}| = |\cos(\alpha) + i\sin(\alpha)| = \sqrt{\cos^2(\alpha) + \sin^2(\alpha)} = 1$$

we see that $|r|^6 = 64$ and hence $r = 2$ since r is a positive real number.

Instructor's Comments: This is the 40 minute mark.

Hence, we see that $-64 = r^6 e^{i6\theta} = 64e^{i6\theta}$ and so $e^{i6\theta} = -1$. Thus,

$$\cos(6\theta) + i\sin(6\theta) = -1 = \cos(\pi) + i\sin(\pi)$$

Hence, this is true when $6\theta = \pi + 2\pi k$ for all $k \in \mathbb{Z}$. Solving for θ gives

$$\theta = \frac{\pi + 2\pi k}{6} = \frac{\pi}{6} + \frac{\pi}{3}k$$

Now, when do two values of θ coincide with the same complex point? Answer: When they differ by multiples of 2π.

Claim: $\theta_1 = \frac{\pi}{6} + \frac{\pi}{3}k_1$ and $\theta_2 = \frac{\pi}{6} + \frac{\pi}{3}k_2$ are equal up to 2π rotations if and only if $k_1 \equiv k_2 \pmod 6$.

Proof: We have that

$$\begin{aligned} \theta_1 &= \theta_2 + 2\pi m && \text{for some } m \in \mathbb{Z} \\ \frac{\pi}{6} + \frac{\pi}{3}k_1 &= \frac{\pi}{6} + \frac{\pi}{3}k_2 + 2\pi m \\ \frac{\pi}{3}k_1 &= \frac{\pi}{3}k_2 + 2\pi m \\ k_1 &= k_2 + 6m \\ k_1 &\equiv k_2 \pmod 6 \end{aligned}$$

and each of the above steps are if and only if steps. This completes the proof of the claim.

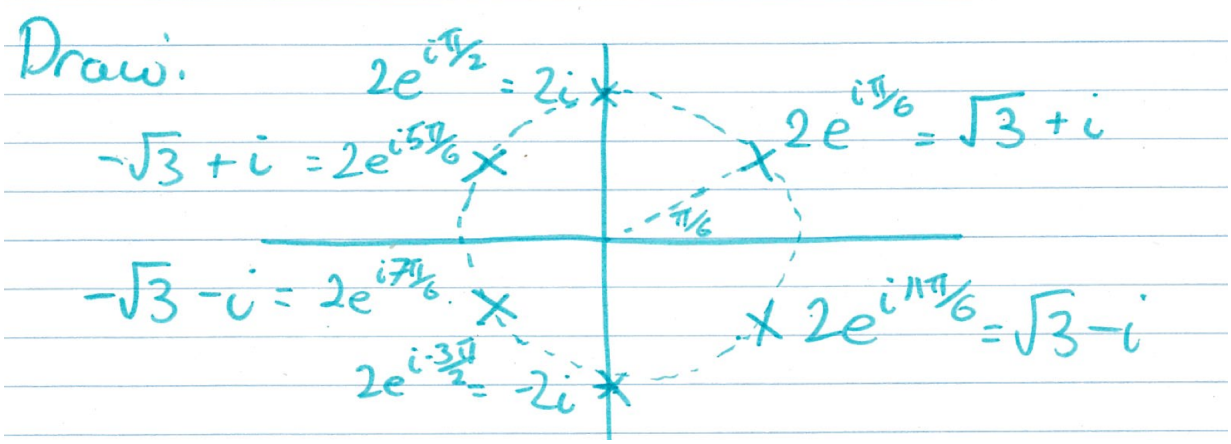
Hence $\theta = \frac{\pi}{6} + \frac{\pi}{3}k_1$ for $k_1 \in \{0, 1, 2, 3, 4, 5\}$. Thus,

$$\theta \in \{\tfrac{\pi}{6}, \tfrac{3\pi}{6}, \tfrac{5\pi}{6}, \tfrac{7\pi}{6}, \tfrac{9\pi}{6}, \tfrac{11\pi}{6}\}$$

or rewritten as

$$\theta \in \{\tfrac{\pi}{6} + \tfrac{\pi}{3}k_1 : k_1 \in \{0, 1, 2, 3, 4, 5\}\}$$

Therefore, $z = re^{i\theta} \in \{2e^{i(\pi/6+\pi k/3)} : k \in \{0, 1, 2, 3, 4, 5\}\}$.



Instructor's Comments: In all likelihood, the 50 minute mark is somewhere above. Carry through to lecture 39 as needed.

Lecture 39

Theorem: Complex nth Roots Theorem (CNRT) Any nonzero complex number has exactly $n \in \mathbb{N}$ distinct nth roots. The roots lie on a circle of radius $|z|$ centred at the origin and spaced out evenly by angles of $2\pi/n$. Concretely, if $a = re^{i\theta}$, then solutions to $z^n = a$ are given by $z = \sqrt[n]{r}e^{i(\theta+2\pi k)/n}$ for $k \in \{0, 1, ..., n-1\}$.

Proof: The proof is like the example yesterday and is left as additional reading. ■

Definition: An nth root of unity is a complex number z such that $z^n = 1$. These are sometimes denoted by ζ_n.

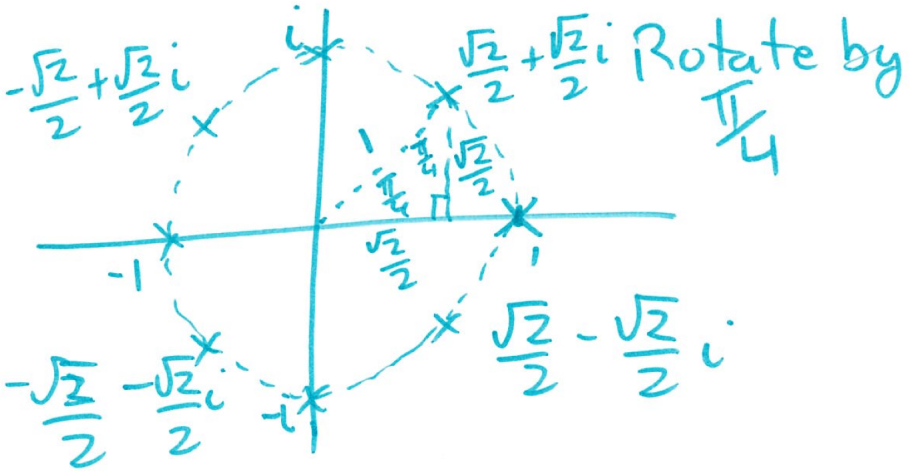
Example: -1 is a second root of unity (and a fourth root of unity and a sixth root of unity etc.)

Instructor's Comments: This is the 10 minute mark; though likely the previous lecture spilled over to this lecture.

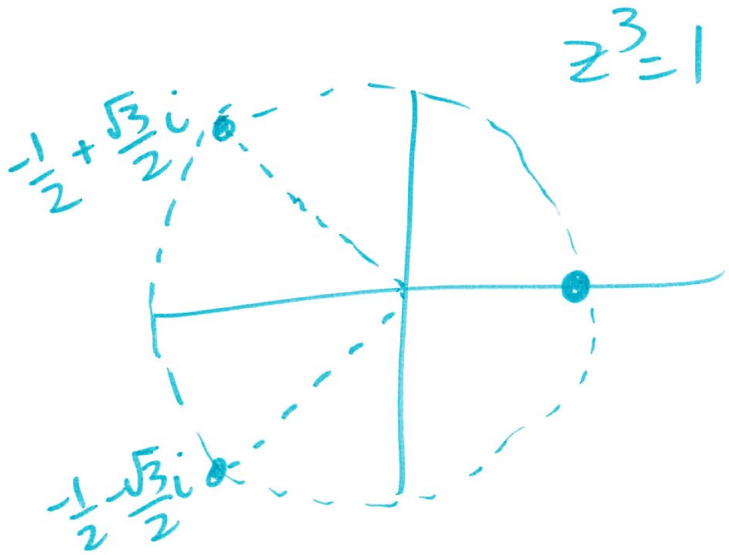
Handout or Document Camera or Class Exercise

Find all eighth roots of unity in standard form.

Solution: We want to solve $z^8 = 1$. We know that $\{\pm 1, \pm i\}$ are solutions. We can draw to find the rest:



For another example, look at $z^3 = 1$:



Example: Solve $z^5 = -16\overline{z}$.

Instructor's Comments: Get students to guess the total number of solutions. Also get them to find a solution by inspection. The answer is surprising!

Solution: This is a tricky problem. One could convert to polar coordinates but I prefer to reason as follows. If I can't solve the equation as written, maybe I can simplify by taking lengths on both sides.

$$|z^5| = |z|^5 = |-16\overline{z}| = 16|\overline{z}| = 16|z|$$

This gives $|z|^5 = 16|z|$. Hence $|z|^5 - 16|z| = 0$ giving $|z|(|z|^4 - 16) = 0$. This gives either $|z| = 0$ which translates to $z = 0$ or $|z|^4 = 16$ which gives $|z| = 2$. So assuming that $z \neq 0$, we multiply the original equation by z to yield

$$z^6 = -16z\overline{z} = -16|z|^2 = -64$$

but this question we solved before! Therefore,

$$z \in \{0, \pm 2i, \pm\sqrt{3} \pm i\}$$

Thus, there are seven solutions!

Instructor's Comments: This is the 40 minute mark; if you spilled over from the previous lecture, this is the 50 minute mark. Otherwise do the next problem (which is one we did before)

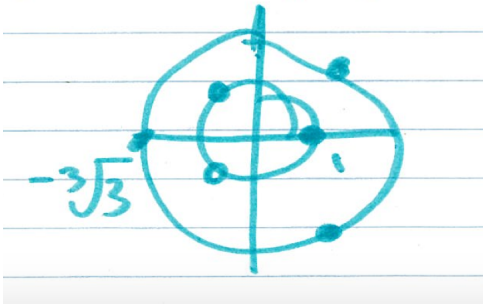
Example: Solve $z^6 + 2z^3 - 3 = 0$.

Proof: From before, we factored this to $(z^3 - 1)(z^3 + 3) = 0$ and thus $z^3 = 1$ or $z^3 = -3$. From CNRT, we see that the solutions to $z^3 = 1 = \cos(0) + i\sin(0)$ are given by

$$z \in \{e^{i\cdot 0}, e^{i\cdot 2\pi/3}, e^{i\cdot 4\pi/3}\}$$

and solutions to $z^3 = -3 = 3(\cos(\pi) + i\sin(\pi))$ are given by

$$z \in \{\sqrt[3]{3}e^{i\cdot\pi/3}, \sqrt[3]{3}e^{i\cdot\pi}, \sqrt[3]{3}e^{i\cdot 5\pi/3}\}$$



This completes the question. ■

Lecture 40

Handout or Document Camera or Class Exercise

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

A) $16i$

B) 27

C) 32

D) -45

E) 64

Solution:

Instructor's Comments: Emphasize there are lots of ways to get the solution.

$$\begin{aligned}\left|\left(\overline{-\sqrt{3}+i}\right)^5\right| &= \left|\left(-\sqrt{3}-i\right)^5\right| \\ &= \left|\left(-\sqrt{3}-i\right)\right|^5 \qquad \text{PM} \\ &= \sqrt{(-\sqrt{3})^2+(-1)^2}^{\,5} \\ &= \sqrt{4}^5 \\ &= 32\end{aligned}$$

Instructor's Comments: This is the 7-10 minute mark depending on how many ways you find the above answer

Polynomials For us, a field will mean to include $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ where p is a prime number. A ring will include the aforementioned fields as well as $\mathbb{Z}$ and $\mathbb{Z}_m$ for any $m \in \mathbb{N}$.

Definition: A polynomial in x over a ring R is an expression of the form

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$$

where $a_0, a_1, ...a_n \in R$ and $n \geq 0$ is an integer. Denote the set (actually a ring) of all polynomials over R by $R[x]$.

Instructor's Comments: We will predominately use fields in the above definition. Some of the theorems we do will only work in the case of fields. For simplicity I will state all the theorems with fields to match the textbook though in many cases, a ring is all you need.

Example:

(i) $(2\pi + i)z^3 - \sqrt{7}z + \frac{55}{4}i \in \mathbb{C}[z]$.

(ii) $[5]x^2 + [3]x + [1] \in \mathbb{Z}_7[x]$. We usually write this as $5x^2 + 3x + 1 \in \mathbb{Z}_7[x]$.

(iii) $x^2 + \frac{1}{x}$ is *not* a polynomial.

(iv) $x + \sqrt{x}$ is *not* a polynomial.

(v) $1 + x + x^2 + ...$ is *not* a polynomial.

Definition:

(i) The coefficient of $a_n x^n$ is a_n

(ii) A term of a polynomial is any $a_i x^i$

(iii) The degree of a polynomial is n provided $a_n x^n$ is the term with the largest exponent on x and nonzero coefficient.

(iv) 0 is the zero polynomial (all coefficients are 0). The degree of the zero polynomial is undefined (some books say it is negative infinity for reasons we will see later)

(v) A root of a polynomial $p(x) \in R[x]$ is a value $a \in R$ such that $p(a) = 0$.

(vi) If the degree of a polynomial is

- 1, then the polynomial is linear.
- 2, then the polynomial is quadratic.
- 3, then the polynomial is cubic.

(vii) $\mathbb{C}[x]$ are the complex polynomials, $\mathbb{R}[x]$ are the real polynomials, $\mathbb{Q}[x]$ are the rational polynomials, $\mathbb{Z}[x]$ are the integral polynomials.

(viii) Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \qquad \text{and} \qquad g(x) = b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0$$

be polynomials over $R[x]$. Then $f(x) = g(x)$ if and only if $a_i = b_i$ for all $i \in \{0, 1, ..., n\}$.

(ix) x is an indeterminate (or a variable). It has no meaning on it's own but can be replaced by a value whenever it makes sense to do so.

(x) Operations on polynomials: Addition, Subtraction, Multiplication (See next page)

Instructor's Comments: This is probably the 25-30 minute mark. The lecture is a bit dry but we need to be on the same page.

Handout or Document Camera or Class Exercise

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

Solution:

$$\begin{aligned}(x^5 + x^2 + 1)(x + 1) + (x^3 + x + 1) &= x^6 + x^5 + x^3 + x^2 + x + 1 + x^3 + x + 1 \\ &= x^6 + x^5 + 2x^3 + x^2 + 2x + 2 \\ &= x^6 + x^5 + x^2\end{aligned}$$

Example: Prove that $(ax+b)(x^2+x+1)$ over $\mathbb{R}$ is the zero polynomial if and only if $a=b=0$.

Proof: Expanding gives

$$(ax+b)(x^2+x+1) = ax^3+(a+b)x^2+(a+b)x+b.$$

This is the zero polynomial if and only if $a=0$, $a+b=0$ and $b=0$ which holds if and only if $a=b=0$. ■

Instructor's Comments: This is the 40 minute mark

Theorem: (Division Algorithm for Polynomials (DAP)) Let $\mathbb{F}$ be a field. If $f(x), g(x) \in \mathbb{F}[x]$ and $g(x) \neq 0$ then there exists unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.

Proof: Exercise (or extra reading). ■

Note:

(i) $q(x)$ is the quotient.

(ii) $r(x)$ is the remainder.

(iii) If $r(x) = 0$, then $g(x)$ divides $f(x)$ and we write $g(x) \mid f(x)$. Otherwise, $g(x) \nmid f(x)$. In this case, we say that $g(x)$ is a factor of $f(x)$. If a polynomial has no nonconstant polynomial factor of smaller degree, we say that the polynomial is irreducible.

Instructor's Comments: Note here that we're generalizing the definition of $|$. This reduces to the definition we had for integers.

Example: Show over $\mathbb{R}$ that

$$(x-1) \nmid (x^2+1)$$

Proof: By DAP, there exists $q(x)$ and $r(x)$ polynomials over $\mathbb{R}$ such that

$$x^2+1 = (x-1)q(x) + r(x)$$

To show that $r(x) \neq 0$, it suffices to show that $r(a) \neq 0$ for some $a \in \mathbb{F}$. Take $x = 1$. Then

$$(1)^2+1 = (1-1)q(1) + r(1)$$

giving $2 = r(1)$. Therefore, $r(x) \neq 0$ hence $(x-1) \nmid x^2+1$. ■

Instructor's Comments: My guess is that you will need to push this to the next lecture which is fine.

Long Division

Let's divide

$$f(z) = iz^3+(i+3)z^2+(5i+3)z+(2i-2)$$

by $g(z) = z+(i+1)$.

$$
\begin{array}{r|l}
 & iz^2 + 4z + (i-1) \\
\hline
z+(i+1) & iz^3 + (i+3)z^2 + (5i+3)z + (2i-2) \\
 & -(iz^3 + (i-1)z^2) \\
 & \underline{\quad\quad 4z^2 + (5i+3)z} \\
 & -(4z^2 + (4i+4)z) \\
 & \underline{\quad\quad (i-1)z + (2i-2)} \\
 & -((i-1)z - 2) \\
 & \underline{\quad\quad 2i}
\end{array}
$$

$\therefore q(z) = iz^2 + 4z + (i-1)$

$r(z) = 2i$

Lecture 41

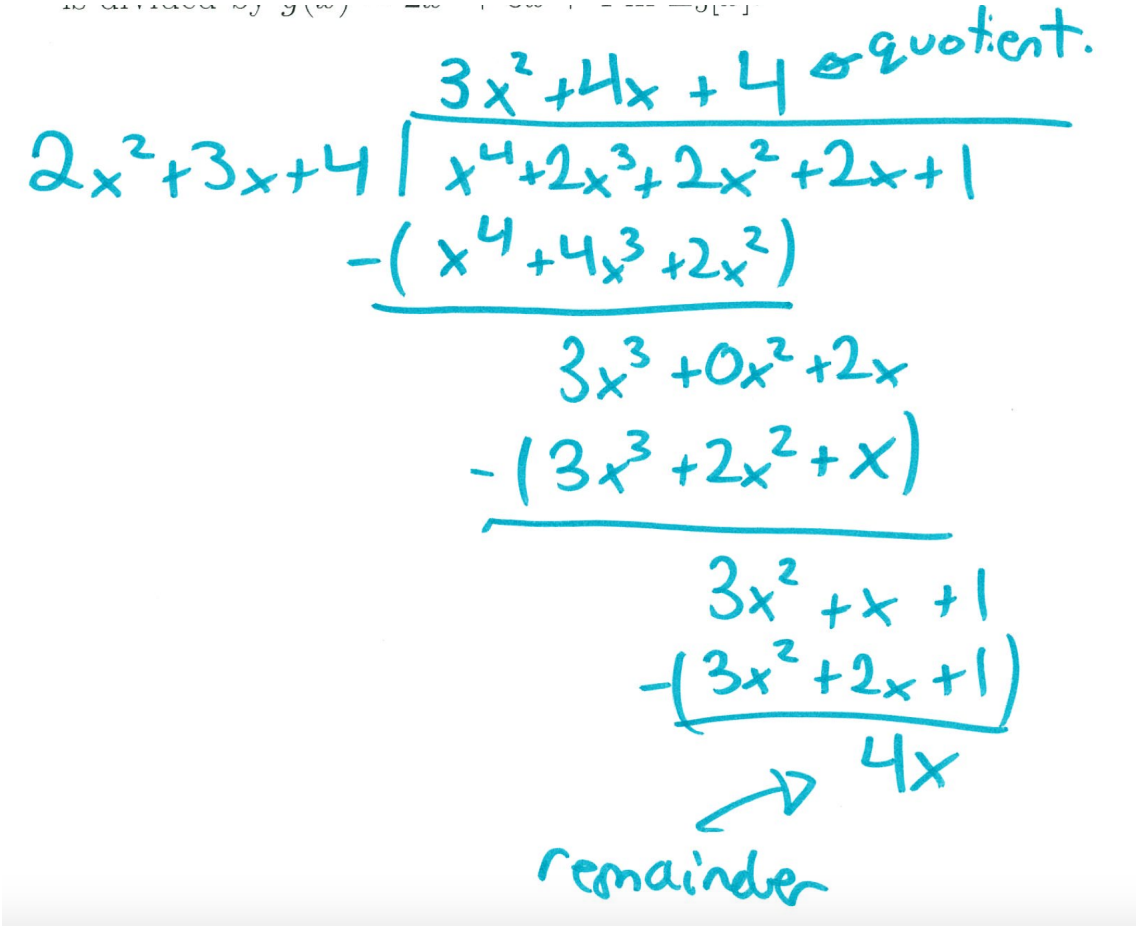
Handout or Document Camera or Class Exercise

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 $\mathbb{Z}_5[x]$.

Solution:



Instructor's Comments: This is the 10 minute mark

Proposition: Let $f(x), g(x) \in \mathbb{F}[x]$ be nonzero polynomials. If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = cg(x)$ for some $c \in \mathbb{F}$.

Proof: By definition, there exists $q(x)$ and $\hat{q}(x)$ in $\mathbb{F}[x]$ such that

$$f(x) = g(x)q(x)$$
$$g(x) = f(x)\hat{q}(x)$$

Substituting the second equation into the first gives:

$$f(x) = f(x)\hat{q}(x)q(x) \quad \Longrightarrow \quad f(x)(1 - \hat{q}(x)q(x)) = 0$$

As $f(x) \neq 0$, we see that $1 = \hat{q}(x)q(x)$. In fact, $\hat{q}(x)$ and $q(x)$ are nonzero. Now, note that $\deg(1) = 0$ and thus

$$0 = \deg(\hat{q}(x)q(x)) = \deg(\hat{q}(x)) + \deg(q(x))$$

(the last equality is an exercise - it holds in generality for nonzero polynomials). Therefore, $\deg(q(x)) = 0 = \deg(\hat{q}(x))$. Therefore, $q(x) = c \in \mathbb{F}$. Thus, substituting this into $f(x) = g(x)q(x)$ gives $f(x) = cg(x)$ completing the proof. ■

Instructor's Comments: This is the 25 minute mark

Theorem: (Remainder Theorem (RT)) Suppose that $f(x) \in \mathbb{F}[x]$ and that $c \in \mathbb{F}$. Then, the remainder when $f(x)$ is divided by $x - c$ is $f(c)$.

Proof: By the Division Algorithm for Polynomials, there exists unique $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that

$$f(x) = (x - c)q(x) + r(x)$$

with $r(x) = 0$ or $\deg(r(x)) < \deg(x - c) = 1$. Therefore, $\deg(r(x)) = 0$. In either case, $r(x) = k$ for some $k \in \mathbb{F}$. Plug in $x = c$ into the above equation to see that $f(c) = r(c) = k$. Hence $r(x) = f(c)$. ■

Example: Find the remainder when $f(z) = z^2 + 1$ is divided by

(i) $z - 1$

(ii) $z + 1$

(iii) $z + i + 1$

Solution:

(i) By the Remainder Theorem, the remainder is $f(1) = (1)^2 + 1 = 2$.

(ii) Note that $z + 1 = z - (-1)$. By the Remainder Theorem, the remainder is $f(-1) = (-1)^2 + 1 = 2$.

Note: $z^2 + 1 = (z - 1)(z + 1) + 2$

(iii) Note that $z + i + 1 = z - (-i - 1)$. By the Remainder Theorem, the remainder is $f(-i - 1) = (-i - 1)^2 + 1 = -1 + 2i + 1 + 1 = 2i + 1$.

Handout or Document Camera or Class Exercise

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

Solution: Since $x+6 = x-1$ in $\mathbb{Z}_7$, we see by the Remainder Theorem that the remainder is

$$4(1)^3 + 2(1) + 5 = 11 \equiv 4 \pmod 7$$

Instructor's Comments: Ideally this is the 40 minute mark.

Theorem: (Factor Theorem (FT)) Suppose that $f(x) \in \mathbb{F}[x]$ and $c \in \mathbb{F}$. Then the polynomial $x - c$ is a factor of $f(x)$ if and only if $f(c) = 0$, that is, c is a root of $f(x)$.

Proof: Note that $x - c$ is a factor of $f(x)$ if and only if $r(x) = 0$ via the Division Algorithm for Polynomials (DAP) which holds if and only if $r(x) = f(c) = 0$ via the Remainder Theorem (RT). ■

Handout or Document Camera or Class Exercise

Prove that there does not exist a real linear factor of

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

Solution: By the factor theorem, it suffices to show that $f(x)$ has no real roots. We will show that $f(x) > 0$ for all $x \in \mathbb{R}$.

Case 1: Suppose that $|x| \geq 1$. Then $x^8 + x^3 \geq 0$ and hence $f(x) = x^8 + x^3 + 1 > 0$.

Case 2: Suppose that $|x| < 1$. Then $|x^3| < 1$ and so $x^3 + 1 > 0$ and hence $f(x) = x^8 + x^3 + 1 > 0$.

Instructor's Comments: Note here that $-1 < x^3 < 1$ and $x^8 \geq 0$. This is the 50 minute mark.

Lecture 42

Handout or Document Camera or Class Exercise

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

Instructor's Comments: If you try this by contradiction, you will find yourself using some sort of " dot dot dot" type argument which ideally we'd like to avoid. Try to steer students to the induction solution.

Solution: Let $P(n)$ be the statement that all polynomials over $\mathbb{F}$ of degree n have at most n roots. We prove this by induction on n.

Base Case: If $n = 1$, let $ax + b \in \mathbb{F}[x]$, with $a \neq 0$. Solving for a root gives $x = -a^{-1}b$ which exists since a is a nonzero element in a field and hence has a multiplicative inverse.

Induction Hypothesis: Assume that $P(k)$ is true for some $k \in \mathbb{N}$.

Instructor's Comments: It's always a good idea to emphasize the for some statement above.

Inductive step: Let $p(x) \in \mathbb{F}[x]$ be a degree $k+1$ polynomial. Either $p(x)$ has no root in which case we are done or $p(x)$ has a root, say $c \in \mathbb{F}$. By the Factor Theorem, $x - c$ is a factor of $p(x)$. Write $p(x) = (x-c)q(x)$ for some $q(x) \in \mathbb{F}[x]$ of degree k. By the inductive hypothesis, $q(x)$ has at most k roots. Thus, $p(x)$ has at most $k+1$ roots. Therefore, by the Principle of Mathematical Induction, $P(n)$ is true for all natural numbers n. ■

Instructor's Comments: This could be the 15 minute mark

Definition: Let $\mathbb{F}$ be a field. We say a polynomial of positive degree in $\mathbb{F}[x]$ is reducible in $\mathbb{F}[x]$ if and only if it can be written as the product of two polynomials in $\mathbb{F}[x]$ of positive degree. Otherwise, we say that the polynomial is irreducible in $\mathbb{F}[x]$. For example, x^2+1 is irreducible in $\mathbb{R}[x]$ but reducible in $\mathbb{C}[x]$.
Example: Factor $f(x) = x^4-2x^3+3x^2-4x+2$ into a product of irreducible polynomials over $\mathbb{Z}_7$.

Proof: Note that $f(1) = 0$ and thus, by the Factor Theorem, $x-1$ is a factor. By long division, we have that

$$f(x) = (x-1)(x^3 - x^2 + 2x - 2)$$

Now, the sum of the coefficients of the cubic is still 0 hence $x-1$ is another factor of $f(x)$! By a second application of long division, we see that

$$f(x) = (x-1)^2(x^2+2)$$

Instructor's Comments: Emphasize to students they should do the long division.

Now, the Factor Theorem says that if x^2+2 could be factored, it must have a root since the factors must be linear. Checking the 7 possible roots gives

$$\begin{aligned}
(0)^2 + 2 &\equiv 2 \pmod 7 \\
(1)^2 + 2 &\equiv 3 \pmod 7 \\
(2)^2 + 2 &\equiv 6 \pmod 7 \\
(3)^2 + 2 &\equiv 4 \pmod 7 \\
(4)^2 + 2 &\equiv 4 \pmod 7 \\
(5)^2 + 2 &\equiv 6 \pmod 7 \\
(6)^2 + 2 &\equiv 2 \pmod 7
\end{aligned}$$

Therefore, x^2+2 has no root in $\mathbb{Z}_7$ and the above form was completely factorized. ■

Instructor's Comments: This is the 20 minute mark. You want to emphasize that even though the factor theorem shows that 1 is a root, it doesn't say with what multiplicity. Thus you need to do the long division in order to find any additional factors (or use the gcd of the polynomial and it's derivative but we won't be talking about this)

Definition: The multiplicity of a root $c \in \mathbb{F}$ of $f(x) \in \mathbb{F}[x]$ is the largest $k \in \mathbb{N}$ such that $(x-c)^k$ is a factor of $f(x)$.

Instructor's Comments: Note we can take $\mathbb{N}$ above because we require that c is a root of the polynomial.

Example: The multiplicity of 1 in the last example was 2.

Note: $x^4+2x^2+1 = (x^2+1)^2$ over $\mathbb{R}[x]$ but does not split into linear factors over $\mathbb{R}$.

Theorem: (Fundamental Theorem of Algebra (FTA)) Every non-constant complex polynomial has a complex root.

Instructor's Comments: The proof will not be done in Math 135

Note:

(i) Roots need not be distinct.

(ii) $x^2 + 1$ over $\mathbb{R}$ shows that this does not happen over all fields.

Example: Solve $x^3 - x^2 + x - 1 = 0$ over $\mathbb{C}$.

Solution: Note that $x - 1$ is a factor (sum of coefficients is 0). Thus, either do long division or note that

$$x^3 - x^2 + x - 1 = x^2(x - 1) + (x - 1) = (x - 1)(x^2 + 1) = (x - 1)(x - i)(x + i).$$

Instructor's Comments: This is the 30 minute mark

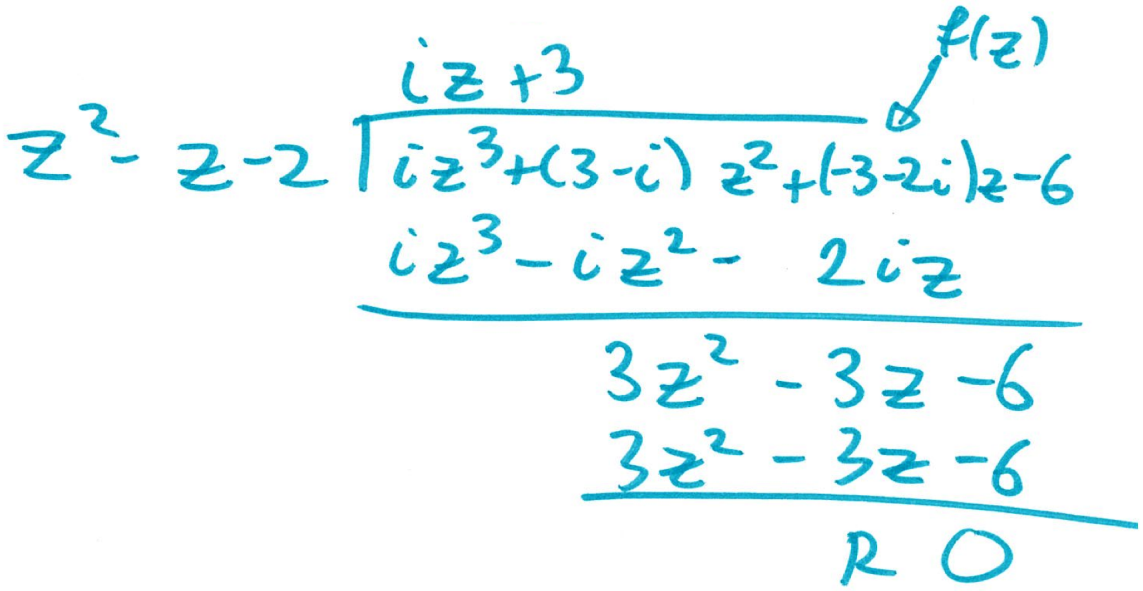
Handout or Document Camera or Class Exercise

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!

Solution: By testing roots, notice that $z = -1$ and $z = 2$ are roots!

Instructor's Comments: Note that you could look at the real part of this polynomial when you plug in a real root r and get $3r^2 - 3r - 6$ which has the two roots -1 and 2.

Hence $(z+1)(z-2) = z^2 - z - 2$ is a factor. Performing the long division yields



and therefore, $f(x) = (z+1)(z-2)(iz+3)$.

Instructor's Comments: Alternatively, you could note that since the constant term of the polynomial is -6, the last linear factor must have $+3$ as its constant term and since the leading coefficient is iz^3, the leading coefficient must be i.

Instructor's Comments: This is the 40 minute mark.

Theorem: (Complex Polynomials of Degree n Have n Roots (CPN)) A complex polynomial $f(z)$ of degree $n \geq 1$ can be written as

$$f(z) = c(z - c_1)(z - c_2)...(z - c_n)$$

for some $c \in \mathbb{C}$ where $c_1, c_2, ..., c_n \in \mathbb{C}$ are the (not necessarily distinct) roots of $f(z)$.

Example: The polynomial $2z^7 + z^5 + iz + 7$ can be written as

$$2(z - z_1)(z - z_2)...(z - z_7)$$

for some roots $z_1, z_2, ..., z_7 \in \mathbb{C}$.

Note: The factorization depends on the field! For example, factoring $z^5 - z^4 - z^3 + z^2 - 2z + 2$...

(i) ... over $\mathbb{C}$, $(z - i)(z + i)(z - \sqrt{2})(z + \sqrt{2})(z - 1)$

(ii) ... over $\mathbb{R}$, $(z^2 + 1)(z - \sqrt{2})(z + \sqrt{2})(z - 1)$

(iii) ... over $\mathbb{Q}$, $(z^2 + 1)(z^2 - 2)(z - 1)$

Instructor's Comments: If you're getting close, it might be best to stop here and continue this on the next lecture.

Proof: (of CPN) We prove the given statement by induction on n.

Base Case: When $n = 1$, take $az + b \in \mathbb{C}[z]$ where $a \neq 0$ and rewrite this as $a(z - \frac{-b}{a})$.

Inductive Hypothesis: Assume all polynomials over $\mathbb{C}$ of degree k can be written in the given form for some $k \in \mathbb{N}$.

Inductive Step: Take $f(z) \in \mathbb{C}[z]$ of degree $k + 1$. By the Fundamental Theorem of Algebra and the Factor Theorem there is a factor $z - c_{k+1}$ of $f(z)$ for some $c_{k+1} \in \mathbb{C}$. Write

$$f(z) = (z - c_{k+1})g(z)$$

where $g(z)$ has degree k. By the inductive hypothesis, write

$$g(z) = c(z - c_1)...(z - c_k)$$

for $c_1, c_2, ...c_k \in \mathbb{C}$. Combine to get

$$f(z) = c\prod_{i=1}^{k+1}(z - c_i).$$

Therefore, by the Principle of Mathematical Induction, the given statement is true for all $n \in \mathbb{N}$. ■

Instructor's Comments: This is the 50 minute mark

Lecture 43

Theorem: Rational Roots Theorem (RRT) If $f(x) = a_n x^n + ... + a_1 x + a_0 \in \mathbb{Z}[x]$ and $r = \frac{s}{t} \in \mathbb{Q}$ is a root of $f(x)$ over $\mathbb{Q}$ in lowest terms, then $s \mid a_0$ and $t \mid a_n$.

Proof: Plug r into $f(x)$:

$$0 = a_n(\tfrac{s}{t})^n + ... + a_1(\tfrac{s}{t}) + a_0.$$

Multiply by t^n

$$0 = a_n s^n + a_{n-1}s^{n-1}t + ... + a_1 s t^{n-1} + a_0 t^n.$$

Rearranging gives

$$a_0 t^n = -s(a_n s^{n-1} + a_{n-1}s^{n-2}t + ... + a_1 t^{n-1})$$

and hence $s \mid a_0 t^n$. Since $\gcd(s,t) = 1$, we see that $\gcd(s,t^n) = 1$ (following from GCDPF) and hence $s \mid a_0$ by Coprimeness and Divisibility. Similarly, $t \mid a_n$. ■

Example: Find the roots of

$$2x^3 + x^2 - 6x - 3 \in \mathbb{R}[x]$$

Solution: By the Rational Roots Theorem, if r is a root, then writing $r = \frac{s}{t}$, we have that $s \mid -3$ and $t \mid 2$. This gives the following possibilities for r:

$$\pm 1, \pm 3, \pm\frac{3}{2}, \pm\frac{1}{2}$$

Trying each of these possibilities one by one shows that $r = -\frac{1}{2}$ is a root since

$$2(\tfrac{-1}{2})^3 + (\tfrac{-1}{2})^2 - 6(\tfrac{-1}{2}) - 3 = \tfrac{-1}{4} + \tfrac{1}{4} + 3 - 3 = 0$$

Hence $(x + \frac{1}{2})$ or $(2x+1)$ is a factor. By long division (or grouping and factoring), we see that

$$2x^3 + x^2 - 6x - 3 = (2x+1)(x^2 - 3) = (2x+1)(x - \sqrt{3})(x + \sqrt{3})$$

Hence all real roots are given by $\frac{-1}{2}, \pm\sqrt{3}$. ■

Instructor's Comments: This is the 15 minute mark.

Handout or Document Camera or Class Exercise

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

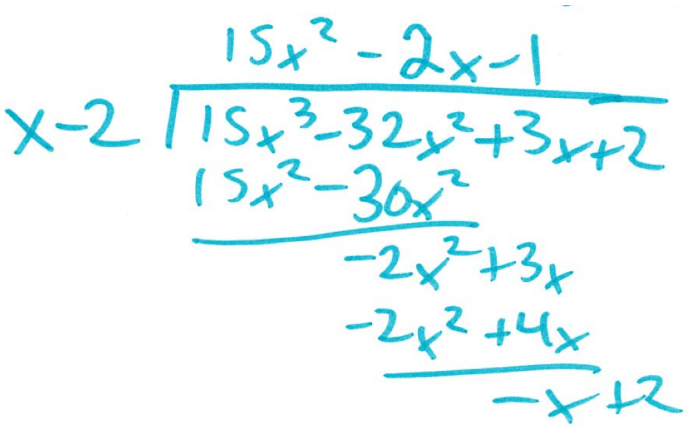
Solution: The above polynomial is equal to

$$\tfrac{1}{15}(15x^3 - 32x^2 + 3x + 2) = f(x)$$

By the Rational Roots Theorem, possible roots are

$$\pm 1, \pm\tfrac{1}{3}, \pm\tfrac{1}{5}, \pm\tfrac{1}{15}, \pm 2, \pm\tfrac{2}{3}, \pm\tfrac{2}{5}, \pm\tfrac{2}{15},$$

Note that $x = 2$ is a root. Hence by the Factor Theorem, $x - 2$ is a factor. By long division:



we have that $f(x) = \frac{1}{15}(x-2)(15x^2 - 2x - 1) = \frac{1}{15}(x-2)(5x+1)(3x-1)$ completing the question. ■

Instructor's Comments: This is the 30 minute mark

Example: Prove that $\sqrt{7}$ is irrational.

Proof: Assume towards a contradiction that $\sqrt{7} = x \in \mathbb{Q}$. Square both sides gives

$$7 = x^2 \qquad \Longrightarrow \qquad 0 = x^2 - 7$$

Therefore, as a polynomial, $x^2 - 7$ has a rational root. By the Rational Root Theorem, the only possible rational roots are given by $\pm 1, \pm 7$. By inspection, none of these are roots:

$$(\pm 1)^2 - 7 = -6 \neq 0 \qquad (\pm 7)^2 - 7 = 42 \neq 0$$

Hence, x cannot be rational. ■

Instructor's Comments: This is the 35 minute mark

Handout or Document Camera or Class Exercise

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

Solution: Assume towards a contradiction that $\sqrt{5}+\sqrt{3}=x\in\mathbb{Q}$. Squaring gives

$$5+2\sqrt{15}+3=x^2 \qquad \Longrightarrow \qquad 2\sqrt{15}=x^2-8$$

Squaring again gives

$$60=x^4-16x^2+64 \qquad \Longrightarrow \qquad 0=x^4-16x^2+4$$

By the Rational Roots Theorem, the only possible roots are

$$\pm 1, \pm 2, \pm 4$$

A quick check shows that none of these work. ■

Instructor's Comments: This is the 45 minute mark

Theorem: (Conjugate Roots Theorem (CJRT)) If $c \in \mathbb{C}$ is a root of a polynomial $p(x) \in \mathbb{R}[x]$ (over $\mathbb{C}$) then $\overline{c}$ is a root of $p(x)$.

Proof: Write $p(x) = a_n x^n + ... + a_1 x + a_0 \in \mathbb{R}[x]$ with $p(c) = 0$. Then:

$$\begin{aligned}
p(\overline{c}) &= a_n(\overline{c})^n + ... + a_1\overline{c} + a_0 \\
&= \overline{a_n(c)^n} + ... + \overline{a_1 c} + \overline{a_0} && \text{Since coefficients are real and PCJ.} \\
&= \overline{a_n(c)^n + ... + a_1 c + a_0} && \text{By PCJ} \\
&= \overline{p(c)} \\
&= 0
\end{aligned}$$

Instructor's Comments: This is the 50 minute mark.

Lecture 44

Handout or Document Camera or Class Exercise

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

Solution: The first statement is true by the Fundamental Theorem of Algebra. The second is false since $x - 1$ is a factor of the cubic polynomial and so there must be a quadratic factor as well. The third is true since $\mathbb{Q}[x]$ forms a ring. The last is false since say $f(x) = x(x-1)(x-2)(x-3)(x-4) + 1$ has no roots over $\mathbb{Z}_5[x]$. Hence the answer is 2.

Recall:

Theorem: (Conjugate Roots Theorem (CJRT)) If $c \in \mathbb{C}$ is a root of a polynomial $p(x) \in \mathbb{R}[x]$ (over $\mathbb{C}$) then $\overline{c}$ is a root of $p(x)$.

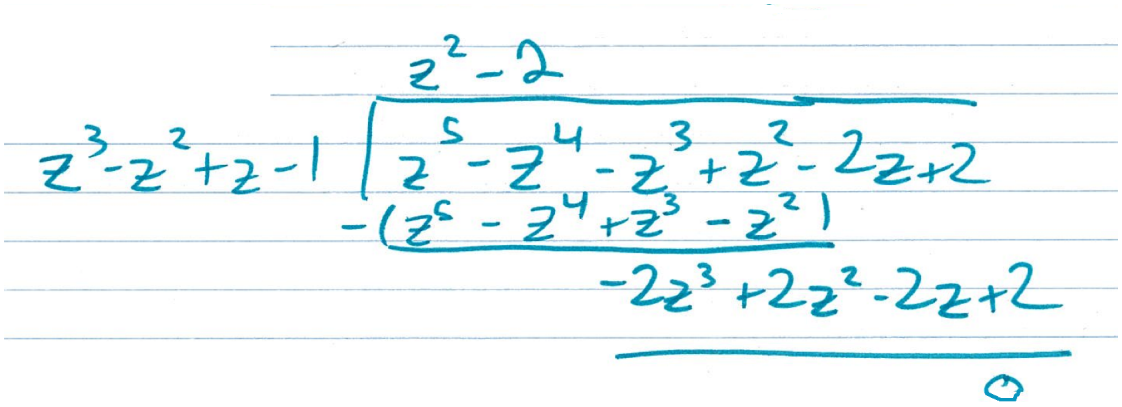
Note: This is not true if the coefficients are not real, for example $(x+i)^2 = x^2 + 2ix - 1$.

Example: Factor

$$f(z) = z^5 - z^4 - z^3 + z^2 - 2z + 2$$

over $\mathbb{C}$ as a product of irreducible elements of $\mathbb{C}[x]$ given that i is a root.

Proof: Note by CJRT that $\pm i$ are roots. By the Factor Theorem, we see that $(z-i)(z+i) = z^2 + 1$ is a factor. Note that $z - 1$ is also a factor since the sum of the coefficients is 0.Hence, $(z^2+1)(z-1) = z^3 - z^2 + z - 1$ is a factor. By long division,



we see that $f(z) = (z^3 - z^2 + z - 1)(z^2 - 2) = (z-i)(z+i)(z-1)(z-\sqrt{2})(z+\sqrt{2})$ is a full factorization. ■

Factor $f(z) = z^4 - 5z^3 + 16z^2 - 9z - 13$ over $\mathbb{C}$ into a product of irreducible polynomials given that $2 - 3i$ is a root.

Factors are (using the Factor Theorem and CJRT)

$$(z - (2 - 3i))(z - (2 + 3i)) = z^2 - 4z + 13$$

After long division,

$$f(z) = (z^2 - 4z + 13)(z^2 - z - 1)$$

By the quadratic formula on the last quadratic,

$$\begin{aligned} z &= \frac{-(-1) \pm \sqrt{(-1)^2 - 4(1)(-1)}}{2(1)} \\ &= \frac{1 \pm \sqrt{5}}{2} \end{aligned}$$

Hence, $f(z) = (z - (2 - 3i))(z - (2 + 3i))(z - (1 + \sqrt{5})/2)(z - (1 - \sqrt{5})/2)$. ■

Theorem: (Real Quadratic Factors (RQF)) Let $f(x) \in \mathbb{R}[x]$. If $c \in \mathbb{C} - \mathbb{R}$ and $f(c) = 0$, then there exists a $g(x) \in \mathbb{R}[x]$ such that $g(x)$ is a real quadratic factor of $f(x)$.

Proof: Let $c \in \mathbb{C}$ be a root of $f(x)$ where $\text{Im}(c) \neq 0$. Then by the Factor Theorem,

$$f(x) = (x - c)q_1(x) \text{ for some } q_1(x) \in \mathbb{C}[x].$$

Now, by the Conjugate Roots Theorem, $\overline{c}$ is also a root of $f(x)$. Hence

$$f(\overline{c}) = (\overline{c} - c)q_1(\overline{c}) = 0.$$

Since $\text{Im}(c) \neq 0$, then $\overline{c} \neq c$, or $\overline{c} - c \neq 0$ which in turn means $q_1(\overline{c}) = 0$. That is, $\overline{c}$ is a root of $q_1(x)$ and so by using the Factor Theorem again, we get that

$$q_1(x) = (x - \overline{c})q_2(x) \text{ where } q_2(x) \in \mathbb{C}[x].$$

We substitute to get

$$f(x) = (x - c)(x - \overline{c})q_2(x) = g(x)q_2(x)$$

where $g(x) = (x - c)(x - \overline{c})$. By Properties of Conjugates and Properties of Modulus,

$$g(x) = x^2 - (c + \overline{c})x + c\overline{c} = x^2 - 2\text{Re}(c)x + |c|^2.$$

Since $-2\text{Re}(c) \in \mathbb{R}$ and $|c|^2 \in \mathbb{R}$, $g(x)$ is a real quadratic polynomial. All that remains is to show that $q_2(x)$ is in $\mathbb{R}[x]$. From above, in $\mathbb{C}[x]$, we have that

$$f(x) = g(x)q_2(x) + r_2(x)$$

where $r_2(x)$ is the zero polynomial. Using the Division Algorithm for Polynomials (DAP) in $\mathbb{R}[x]$, we get

$$f(x) = g(x)q(x) + r(x)$$

where $q(x)$ is in $\mathbb{R}[x]$ and the remainder $r(x)$ is the zero polynomial or $\deg r(x) < \deg g(x)$. Now, every real polynomial is a complex polynomial, so we can also view this as a statement in $\mathbb{C}[x]$. As for any field, DAP over $\mathbb{C}$ tells us that the quotient and remainder are unique. Therefore $r(x) = r_2(x)$ is the zero polynomial and $q(x) = q_2(x)$ has real coefficients.

Handout or Document Camera or Class Exercise

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

Solution: Assume towards a contradiction that $p(x)$ is a real polynomial of odd degree without a root. By the Factor Theorem, we know that if $p(x)$ cannot have a real linear factor. By Real Factors of Real Polynomials, we see that

$$p(x) = q_1(x)...q_k(x)$$

for some quadratic factors $q_i(x)$. Now, taking degrees shows that

$$\deg(p(x)) = 2k$$

contradicting the fact that the degree was of $p(x)$ is odd. Hence, the polynomial must have a real root. ■