Theorems proven during video sessions:

End of Semester

3.11

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ where the a_i and n are integers with $n \geq 0$. Suppose $a \equiv b(\text{mod } m)$ for integers a, b and m, with $m>0$. Prove $f(a) \equiv f(b)(\text{mod } m)$.

3.13

Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$ is a polynomial of degree $n > 0$ with integer coefficients with $a_n > 0$. Then there is an integer k such that for all $x > k$, $f(x) > 0$. (Note: We are only assuming that the leading coefficient a_n is greater than zero. The other coefficients may be positive or negative or zero.)

First Day

1.1

Let a, b, and c be integers. If $a|b$ and $a|c$ then $a|(b + c)$.

Developing a sense of Proof

1.2

Let a, b, and c be integers. If $a|b$ and $a|c$, then $a|(b - c)$.

1.3

Let a, b, and c be integers. If $a|b$ and $a|c$, then $a|bc$.

1.18

A natural number that is expressed in base 10 is divisible by 3 if and only if the sum of its digits is divisible by 3.

Awkward Moments

1.4

Can you weaken the hypothesis of the previous theorem and still prove the theorem? Can you replace the conclusion of the theorem by $a \mid \frac{b}{c}$ and still prove the theorem?

1.21

Division Algorithm: Let n and m be natural numbers. Then there exist integers q (for quotient) and r (for remainder) such that $m = nq + r$ and $0 \leq r \leq n-1$

Difficult Proof

3.15

Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$ is a polynomial of degree $n > 0$ with integer coefficients. Then for infinitely many integers x, $f(x)$ is a composite number.

End of Semester Proof

3.11

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$
$$f(a) = a_n a^n + a_{n-1} a^{n-1} + \dots + a_1 a + a_0$$
$$f(b) = a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0$$

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$$
$$a^{n-1} - b^{n-1} = (a-b)(a^{n-2} + \dots)$$

$$f(a) - f(b) = a_n(a^n - b^n) + a_{n-1}(a^{n-1} - b^{n-1}) + \dots + a_1(a-b)$$
$$f(a) - f(b) = a_n(a-b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1}) + a_{n-1}(a-b)(a^{n-2} + a^{n-3}b + \dots + ab^{n-3} + b^{n-2})$$
$$+ \dots + a_1(a-b) \quad - \text{(1)}$$

Let $k_n = a_n(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$, $k_{n-1} = a_{n-1}(a^{n-2} + a^{n-3}b + \dots + b^{n-2})$

$k_1 = a_1$

Now $a_n, a_{n-1}, \dots, a_1, a, b \in \mathbb{Z}$ $\therefore k_n, k_{n-1}, \dots, k_1 \in \mathbb{Z}$

From (1)

$$f(a) - f(b) = (a-b)[k_n + k_{n-1} + \dots + k_1] \quad \text{——} \quad \text{(11)}$$

Now let $p = k_n + k_{n-1} + \dots + k_1$

$k_n, k_{n-1}, \dots, k_1 \in \mathbb{Z}$ $\therefore p \in \mathbb{Z}$

We also have

$a \equiv b \pmod{m}$

i.e. $m \mid a - b$

$\therefore$ $a - b = mk$ for some $k \in \mathbb{Z}$

From (11)

$f(a) - f(b) = mkp$

$\because$ $m, k, p \in \mathbb{Z}$ $mkp \in \mathbb{Z}$

$m \mid \{f(a) - f(b)\}$

$f(a) \equiv f(b) \pmod{m}$ $\boxtimes$

3.13

PROOF: Let a term of $f(x)$ be $-a_{n-j}\,x^{n-j}$ where $|-a_{n-j}| > a_n x^j$ for some x. Since $|-a_{n-j}|$ is constant and $a_n x^j$ is increasing as $x \to \infty$, there will be some x_m s.t. $|-a_{n-j}| < a_n x_m^j$. So $(a_n x_m^j)(x_m^{n-j}) > |-a_{n-j}\, x_m^{n-j}|$

$\Rightarrow a_n x_m^n > |-a_{n-j}\, x_m^{n-j}|$ for all $x \geq x_m$.

Finding such an x such that the initial term is greater than it. Let the set A be the set of these values of x. So let $k-1 = \max A$. Since $a_n x^n$ is increasing and positive for $x > 0$ $f(x) > 0$ for $x > k$ $\therefore$

End of Semester

Mike: Okay so why don't we go ahead and start with R right now. R, what are you going to tell us?

R: I'm trying to prove 3.11. Uh, it says f(x) is a polynomial of degree n with integer coefficients that means, which I'll be also using later, a_n, a_{n-1}, a_1, a_0 are all integers and we need to prove that if a mod b, a congruent to b mod m then function of a congruent to function of b mod m. So I write down the polynomial and so plug in x equal to a so that becomes polynomial in a and f(b) polynomial in b. Then I've subtracted them, subtracting f(a) from f(b) or f(b) from f(a). So then it gives me a polynomial, this and using the algebra that a^n --

Mike: -- R, R, you've miswritten no, no, right, right there f(a) minus f(b) the very first term. It shouldn't be --

R: -- Oh okay.

Mike: Right. You wrote, the next one's okay it's just that first one you.

R: Yeah. So using the algebra, a^n minus b^n we can write down a-b then this polynomial. Right? Okay. So then, I have tried to use this polynomial like uh, in every term, so that also write down a^{n-1} minus b^{n-1} is equal to a-b, a^{n-2} plus blah, blah, blah. So after that I found out that a_0 minus a_0 cancels out and so finally the last term becomes a_1, a-b. Then I think after that the proof is very easy just to try to use some variables. I tried to use k_n is equal to a_n and then all the terms except a-b, k_{n-1} all the terms except a-b, and then k_1 is equal to a_1. Now all these are integers because it is supposed. And it is also supposed that all of the coefficients are integers. So a_n, a_{n-1}, a_1 be an integer. That means k_n, k_{n-1} integer also. Right? Because all are integers. Okay. And from 1 I just substituted k_n, k_{n-1} for all these terms and then using another variable let p equal to k_n so and since k_n, k_{n-1}, k_1 individual integer so p also an integer. And we also know, and this is the biggest supposition, assumption, a congruent to b mod m which means m divides a-b. That means that a-b is equal to mk for some k an integer. And this is our equation of 2, from 2 I've tried to substitute it all the variables with all the terms in terms of k and p, and m. So f(a) -f(b) is equal to mkp and since m, k, p integer so mkp also integer. That means m divides f(a)-f(b) which implies f(a) is congruent f(b) mod m. And this proves the theorem number 3.11. Any questions?

P: Looks very good; looks just like mine actually.

R: Well yeah. I tried to use lots of variables. I think the proof becomes evident just here, just then.

T: So that k right there is that the same k as the one down there or is it the same one?

R: Which one?

T: K where a-b equals mk on the second column. Is that the same k or a different k?

R: Oh. Well I have written, no, I think it's different k because these are all k_n up to k. I have not tried to use any where like k. So it's different variable. Clear 3.11?

B: I was going to say, I follow you, and I was thinking maybe like in the spirit of the chapter we're doing, could you do this by induction by proving it's true for n=1. Supposing it's true for --

R: N is equal to 1?

B: Right and then supposing it were true for some larger and then just by, you could use the property that you can, if you add two things that are congruent to the same mod.

R: So you're saying n is equal to 1 that means f (x) becomes a_n + a_{n-1} up to a_0. Or m is equal to 1?

B: I mean it's obvious that if you started out with 0, a_0 is congruent to a_0 mod anything.
R: Right.
B: Then if you say let it be true for some n minus 1, greater than 0, you could show that it were true for n.
R: So you're saying that.
B: Just by adding the nth term.
R: For m=1, a mod b mod 1.
Mike: I think n, right? N, the exponent, the exponent. The degree of the polynomial.
R: Oh.
B: I just, I mean, I follow what you're doing I just with the, the expansion I had a hard time keeping the terms straight.
R: Yeah, I think.
B: We have that property that we can add things together. Suppose k were just 0.
R: So.
B: k_0 is a_0, that's a_0.
R: k_0, with integer coefficients. So that means the first case should be k is equal to 0?
B: Yeah, if you just start off with your base case k=0, well then obviously--
R: -- So then the theorem would be defined as n greater than 0 --
Mike: -- Well, well actually, maybe the thing to do here B is why don't you do it by induction right now, but before you do let's ask other questions of R's proof to make sure everyone's followed R's proof and then you can do it by induction to see an alternative method. Do other people have questions about R's proof?
R: Yes?
K: You have, on the second column, you have from 2 uh f(a) -f(b) is mkp, where's the k there come from?
R: Because a is congruent to b mod m so a-b is equal to m times k some integer. And this k is distinct from all these k's sub whatever. Uh, by the definition of congruence like m divides a-b --
K: -- Yeah, I followed that, but a and b are different from f(a) and f(b).
R: Right, but we are given a is congruent to b mod m. So from the definition m divides a -b so a-b is equal to mk for some k integer. And then I have tried to use the form from equation number 2. This is equation number 2.
Mike: Most of us would call that eleven.
(Class laughs)
Mike: Ah, I was wondering why he kept calling it 2. And then I was wondering why did he go 1 and then 11.
(Class laughs)
Mike: You see it K?
K: Yeah.
R: Any confusion?
K: I got it now.
R: Okay. So eleven was confusing.
Mike: W?
W: What is the symbol here on the second line of your second column, before the m divides a-b.
Mike: I-E.

W: Oh, okay.
Mike: It's, it's yeah i.e. I-E.
(Class laughs)
Mike: I.e. comma. Any further questions for R? Okay, that sounds great. Um.
R: And do I need to, I think it's clear from 3.11 that 3.10 follows.
Mike: Oh, yes, yes, 3.10 follows because in fact a and b are congruent to the same thing mod--
R: -- Yeah, 99.
Mike: -- 99. Very good. An.?
An.: I just have, like on 3.10 like uh, theorem 3.11 said like if a is congruent to b you can assume f(a) congruent to f(b) we don't prove that f(a) congruent to f(b) mod m is equal to a congruent to b. So I don't understand why we can go that way. Understand the question?
R: I suppose, so 98, this is true right?
An.: That's true, yeah.
R: So from the theorem doesn't it follow that f(98)?
An.: Yes.
R: So that is what we are supposed to prove. Yes?
K: But you can't use 3.11 in 3.10.
R: Okay, yeah, I know but it is the same thing that you just start with f(98) and f(-100).
P: The spirit of the proof.
Mike: Well he can because he proved it.
K: Oh.
(Class laughs)
Mike: Sure, he actually proved it. As long as you prove it first all is fair. In mathematics all is fair.
C: I took a page and a third on that and then I did this.
Mike: Yeah, but no that's good because the point is, the reason it's in that order is because you understand, you try to understand it with the actual numbers and then this is the generalization. In this case maybe the generalization is easier to deal with.
(Class laughs)
Mike: But that's also what happens, so I think that's fine. I'm not at all apologetic, C, I think, I hope you enjoyed it.
C: I did enjoy it.
Mike: Okay.
C: I did enjoy it, I look forward to the next one.
Mike: I look forward to the next one. R, anything further on, for you? Any questions for R?
R: Any further questions? That means easy proof.
Mike: Okay, very good, let's see we have eight minutes here. I'd like to, I would like to see the induction thing, B.
B: I can just talk through it.
Mike: Just talk through it, just give us a hint about it, an outline.
B: You just take your base case, this is my guess how you'd approach it, and you'd say okay suppose n=0. Well in that case then f(x) is always equal to a_0. So I mean it's simple to prove well f(a) is equal to a_0 which is equal to f(b). So f(a) has got to be congruent to

f(b) mod anything. And then you say okay well assume that it's true for n-1. And so then you just re-write this instead of having k here you'd start with a_{n-1} x^{n-1} and so on plus a_0 at the end. And now we just need to prove that it's true for n. Uh. So we know that, we're given that a is congruent to b mod m. Well from our theorems from chapter one we can say that this is true. And then multiplying by any constant is true. Maybe these should be, yeah these should be, no I'm good.

Mike: Put a congruent sign instead of equal.

B: Yeah, there you go. And multiplying by any constant is true, so let that constant be x to the n.

Mike: Well it's actually a_n.

B: Oh, whoops.

Mike: Is the constant.

B: Is the constant. So the constant is out here like this. And then you just add this and this and by our theorem from chapter 1 again where we can add two things that are congruent to the same mod m.

An.: 1.1.

R: 1.1.

B: Oh, okay. Uh, so.

Mike: Good, good, that's a good outline of an inductive proof of this same thing. Did people follow that? That strategy there? I think it's good to see, to see alternative strategies and also, by the way, I think it's very good to get to the point on induction that you can see how to formulate an inductive argument like B just did, clarifies a particular.

---NEW CLIP---

S: Sure.

T.A.: So let's look at 3.13 by S.

S: All right, okay, so I didn't right the whole thing for space but you have it on your packet. So uh, you have a polynomial where an is greater than 0. Um, all n coefficients are integers. So pick a term, we'll call it $-a_{n-j}x^{n-j}$ where the absolute value of that that term is greater than a_nx^j for some values of x. Um, since that uh, negative, since this is a constant, we know that it will never increase. But this is an increasing function so we know that for some value there will be an x sub m such that this constant will be less than $a_mx_m^j$. Um, so we can uh multiply, we can say, we can multiply this be x_m^{n-j} and show it is greater than the absolute value of that term. And multiplying them together we have $a_mx_m^n$ is greater than the term for all x greater than x_m. Finding such, and we can find such a value for comparing the initial term to every other term so finding a value for which the initial term is greater than every other term. So we can put all those values together in a set we'll call A. And the maximum of that set we'll call k-1. Um, so at this point k-1 will negate every single, will assuredly negate every single term. Uh, uh, k-1 will assuredly, uh. $a_n(k-1)^n$ will negate every single term assuredly. Um, so then since a_nx_n, x^n, is increasing and positive um for x greater than 0 then we know that f(x) is greater than 0 for x greater than k. You follow? Yes?

W: When you say negate you mean become negative?

S: It will overcome or cancel out, it will be bigger. Not negate, sorry. That was poorly. Yes?

V: Okay, what about at the top where it says the absolute value of negative a^{n-j} is greater than an x^j for some x.
S: Mm-hmm.
V: For some x.
S: Yeah.
V: What does that mean?
S: That means there, for some, maybe I should have said for some values of x it will be the case that. We are, we are pulling out terms where the coefficient is larger than.
W: Than the initial term?
S: Yeah.
V: Okay.
S: Uh, we have like, you have like 1 times x^n plus negative 1,000, er, sorry x_n minus negative 1,000 x^2. Where you have a coefficient that is much larger than the other one. So.
V: Okay, so you're saying that the coefficient remains constant but $a_n x^j$, where j is n minus whatever, is the number of that term that we're talking about?
S: Um, no x^j I pulled out for convenience because when you multiply x^j by x^{n-j} you get x^n.
V: Right, right, okay.
A: So what you're doing at the end would imply that an x^n would be greater than the sum of all the other coefficients. But will that be the case or will it be greater than the greatest a_i?
S: It will be greater than the sum of all of the uh.
A: I'm not sure that that's what this implies.
S: Mm.
T.A.: Do you all understand what he just asked? Could you repeat it again what you're saying and.
A: Okay so I'm not sure --
T.A.: -- And what you're, and again your impression of what she's.
A: Yeah, okay, I'm not sure exactly what's done over here but it's kind of, you know if you take an x^n then it will be greater than any other $a_i x^i$. But I'm not sure if that implies that an x^n is going to be greater than the sum of all of the others $a_i x^i$.
S: That's a good point.
T.A.: I see nodding, does that mean people understand or should we say it one more time?
Student: Got it.
T.A.: What do people think?
Al.: Say it one more time.
T.A.: All right.
A: Okay, so this is what I think again. That doing this would prove that an x^n is greater than the largest $a_i x^i$, but it's not larger than all of the $a_i x^i$ put together. Basically, if you take a summation of $a_i x^i$ from i going from n-1 to 0 then it's not going to be.
T.A.: So you're saying what she has says that this term will be greater than the absolute value of the largest.
A: Yeah.
T.A.: You'll find an x such that this term will be larger than the absolute, the largest absolute value of each of these. So you go through and let's say negative a million is one

of the coefficients and when you take the absolute value that's your biggest one. But you're saying that doesn't necessarily assure that if you add up all the absolute values this is bigger than it, is what you're saying?

A: That's what I think.

S: I think I never spotted that, but that's a very good point.

T.A.: What do you think M?

M: What A is saying, I think it's true.

T.A.: That that's, that might be a problem?

M: Yeah.

S: Yes.

C: Well I'm not sure I exactly understand your logic, but I'm okay with that. But to fix this, to fix this, what you'd need to show, ha, all you'd need to show.

(Class laughs)

C: Is that your greatest number times n, since there are n terms over there, that your left term is bigger, that's all you'd have to show because that would assuredly be bigger than all the left-hand, all the right terms.

A: But there's not guarantee of that, you can't just take n because then you can't find an x that way.

D: What do you mean? Why can't you just multiply it by n?

A: Well you can but then how are you going to find the x?

S: Yeah, that's. That won't be necessarily true.

C: Well I thought the proof doesn't ask you to find the x, it just says that there is an x.

A: Yeah but I talked to Dr. Starbird and he said that we should kind of give an estimate of where the x is.

(Class laughs)

T.A.: It's always about him.

(Class laughs)

T.A.: Should we look at M's and see how he addressed this issue? See what you all think of his? Good job S, no one else had a proof.

K: I can do my presentation of theorem 3.15 now.

T.A.: Wait until Marcel does 13.

(Class laughs)

First Day Proof

By def For some integers k & j

$ak = b$ and $aj = c$

$b + c = ak + aj$

$b + c = (k + j)a$

$\frac{b+c}{a} = k + j$

$(k+j)$ is the sum of two integers

First Day

Mike: So um, so in fact let me just talk about, well we talked about the divisors of numbers. Right here, you know I said if you take the divisors of 6 that are less than 6 and uh, you wanted to add them up then you got the number. That was the definition of perfect number. But actually one thing I didn't say is well what is, what is a divisor? What's a divisor? So let's think about this. Suppose that I take two integers. So some integer n and another integer d. D for divisor, n for number. N is a number, d is a divisor. Okay? And I say d is a divisor of n. So what I'd like you to do is talk to somebody next to you. Introduce yourself; say what your name is to them and formulate a definition of what you want to mean by the fact that d is a divisor of n. It's a very simple concept. You all know what it means you know in your heart. Can you write down a definition that actually captures what you know that, that phrase means. That d is a divisor of n. Okay? So talk to each other and I'm going to come around and introduce myself to everybody.
(Students talking)
Mike: So what is your name?
S: S.
Mike: Hi, nice to meet you.
(Students talking)

Mike: I'll ask some people whose names I don't know. Oh first I'll review the names just to impress you. So this is A, don't tell me. A, B, S, Je., S again. By the way so if you have to make a guess, guess S. Because we've got three of them in the room.
(Class laughs)
Mike: There's S, this is S, this is S. So the, the mode is S. Okay. Okay, and so this is Je., this is Ju., this is L, Tr., All., V, J, O, W, Z, and Ai. Okay, so this is it, but I didn't get to other people. So that's all right. Now, so I'll ask some other people for both your names and what you propose as the definition of d is a divisor of n. Okay, so let's maybe, how about this area here. You, what's your group? What was your group? You four were a group?
K: Us two.
Mike: You two and you two were a group. Okay, so what are your names and what was your proposed definition for d is a divisor of n. Uh, and so what are your names.
St.: I'm St.
Mike: St. Okay, hi St.
St.: Hello.
C: I'm C.
Mike: C. Okay, St. and C. Who's the spokesperson for the St. and C?
C: I guess I am.
Mike: All right, C is.
C: We're going to say d is a divisor if n, d, and n over d are all integers.
Mike: Okay, so say it again.
C: D is a divisor.
Mike: D is a divisor of n. This is what you mean?
C: Uh-huh.
Mike: Okay.
C: If n, d.

Mike: N times d?
C: No, n. The number n, the number d.
Mike: Okay. Oh, I see.
C: N comma d and n over d are integers.
Mike: Are integers. Okay. And so by the way to make this complete we should say suppose that d and n are integers. So d and n are integers. Then you're saying that d is a divisor of n if, and by the way, if this is true. Now is that the only condition in which you want to call d a divisor of n, by the way? Are there other, are there other situations in which you'd want to say that d is a divisor of n? What do you think O?
O: N over d may have to be an integer but n and d separately don't have to be.
Mike: Ah-ha. You might want to talk about a category other than just natural numbers. Well that's an interesting thought. Um, what I was thinking about was you want to say if and only if. So this, by the way, is a stock mathematical phrase. What it means is that, that is the only circumstance under which you are going to say that d is a divisor of n. So that's, so when you're making a definition what you're really saying is that whatever it is you're defining is exactly equivalent to whatever it is the definition is. And so you're saying if and only if, means if that definition is true then you want to say that d is a divisor of n and if d is a divisor of n then that thing is true. So if and only if just means they are exactly equivalent to each other. And that's what you want from a definition. So that's just a technicality. Let's now get back to your proposal. So, so, C and St. then have proposed that d is a divisor of n means that n, d, and n over d are all integers. So, let's uh, let's first stick, before we go into O's question, let's stick to the question where we're in the category of n and d being integers and ask the question what do you think of this definition? Is it a good definition? Or would you prefer a different definition? First of all, do you think it's correct in your heart? Is this what you mean by d is a divisor of n? Okay? So let me meet some other people. How about you two? What are your names?
Mi.: Mi.
Mike: Mi., okay.
Jm.: Jm.
Mike: Je. again?
Jm.: Jm.
Mike: Jm., Jm., Jm., okay. So Jm. and Mi. So what do you two think about whether or not this is what you mean, just don't worry about technicalities. I mean is this really what you mean when you say d is a divisor of n?
Jm.: I would agree.
Mike: You would agree. Mi.?
Mi.: Yeah.
Mike: You would agree, okay. Uh, can, could you phrase this instead of, one problem with this that I have is that it introduces the concept of division, and I'd rather if it were possible, I'd rather have a definition that didn't use division. The reason is that division has the potential to take us out of the category of integers. And so it worries me a little bit, you know. It's not wrong; I'm not saying it's wrong. I'm just saying that I'd prefer a definition that doesn't use divide, that doesn't use division. Does anybody have a definition that doesn't use division? Okay, great. Would you introduce yourself?
Da.: Da.
Mike: Da., I'm sorry.

P: I'm P.

Mike: P. Da. and P. Da., Da.

Da.: We said that there exists some x where x times d is equal to n and x, d, and n are all integers.

Mike: Okay, so your proposed definition is this one. Da., uh, uh, so this is Da. and P, if and only if, d is a, d and n are integers then d is a divisor of n if and only if, say it again.

Da.: There exists some x, such that x times d is equal to n.

Mike: There exists some, and then you're going to make x a?

Da.: Integer.

Mike: Integer. So I'll just put it here, there exists some integer x. And in fact I'm not going to use x, I'm going to use k. Such that.

Da.: K times d equals n.

Mike: Right, okay. Okay. Now this is a good definition. This is a good definition too by the way. Perfectly good definition. But this is a good definition and I'll tell you why this is a good definition. This is a good definition because if you have the situation in a hypothesis that d is a divisor of n, then you know something that you can use. Namely you can say oh that means that there must be some integer k so that k times d is equal to n. And that might be a useful existence. A useful thing to, to have in trying to prove something. For example, I'm going to be handing out a list of theorem statements for you in just one minute and the first theorem on here that I'll ask you to prove is this. Suppose a, b, and c are integers. If a divides evenly into b, a is a divisor of b, and a is a divisor of c, then a is a divisor of b+c. So here's, here's the theorem. Let's do this, this is theorem 1.1. Let's just start right now. Theorem 1.1, suppose a, b, and c are integers and. By the way, I'll introduce some notation here. D is a divisor of n is written d divides n. See, and suppose a divides b and a divides c, then a divides b+c. Okay? So go ahead and try to prove that on your own right now. You can talk to the person next to you if you want. But write down the proof that that is the case. You have a number a that divides evenly into b and it also divides evenly into c, then why does it divide evenly into b+c? While you're doing that I'll pass some things out. Could you just pass these down? By the way, I don't hear anything which is a bad sign. I'd like you to be talking to each other, so otherwise you're not going to get to know each other.

Mike: Does somebody have a proof of this theorem? Somebody have a proof? How many of you feel that you have a proof of the, of this theorem? That you can prove it? Okay, put your hand way up if you feel that you can prove this theorem. Okay. Okay, so let me ask. I'll pick somebody at random to, to uh, to do this. Well do I have a volunteer who would like to present your proof? Maybe somebody from the back? You two want to do it? You can both come up. Talk it over in case there's a problem. Here, come here. Okay that's good, that's good. This is An. and T, right?

T: How's it going?

Mike: Okay, An. and T. Now just go ahead and write it down here while I talk. Let me explain what is going to happen in this class. What I just handed you is a list of theorem statements and definitions and you'll see that this, this one is theorem 1.1. It's just the statement, it doesn't have any proof. Your job, your standing job is to figure out, on your own, the proofs of these theorems and to both write them down. Write them down, that's your homework assignment is to write down. The theorems, they're all here so you've got your homework for the whole semester. I'll give, I'll give more notes to you, by the way, as we go through the semester. But these are the first ones. So this will take us through the, for several weeks that you'll be working on these theorems. You'll prove them yourself and then you'll turn them in. Now, when you start today, at least I hope that you're a little unsure. Well what is a proof? I don't know I've never proved anything in my life maybe. You know. And uh, so you don't really know what you're doing. That's fine, that's the way it should be. That's the whole point of this course is to get you accustomed to proving things and learning how to actually produce mathematics on your own. I'd like to think of this course as being a course in which you will, mathematics will change from being a noun to a verb. Right? It's, mathematics is something you do, it's an active thing. It's not just something that comes to you and that you learn. So what your job is, your standing job, and I've written it down here on the, on this other first day handout piece of paper. Your job is to first prove all the theorems on your own, write them up, and present them in class. So everyday in class, like next time which is Friday, what's going to happen is that you're all going to come here in class and I'm going to say to somebody, I'll just pick somebody at random, um like Jm.? I'll say Jm. would you please present your proof to theorem 1.2? And then Jm. will come to the board and will present a proof. Now, now don't sit down. Here, come here. Uh, uh, and what they will do is present the proof like, like will one of you two go ahead and present or both. Go ahead and present. This will be a good sample of what's going to happen. So go ahead.

T: So the theorem is suppose a, b, c, are integers and a divided by b, and a divided by, I mean uh, b divided by a and c divided by a, then b+c is divisible by a also. So we're saying that for some integers k and j, because this is by definition, what we just defined over there, of what uh, uh, that actually means over there. So ak = b and aj = c. And then so then b+c just basically is ak + aj. Then factor out an a over there. And then bc divided by a is just k+j and since both are integers then it's still, it's divisible by a, b+c.

Mike: Okay, now, now. This is a good model. So what we're going to do is then ask people, I'll ask everybody in the class do you think that this is a, an iron clad? Is this a completely correct proof or not? See and it's up to you individually to decide whether or not this is a convincing argument. Remember mathematics is a human constructed idea and something is correct not because it appears in a book, not because it is a you know somebody who is an authority told it to you, but because you are personally convinced by the logic of the reasoning. So then it's your job to look at this logic and say is it in fact, is that ironclad, is this correct. So do, does anybody have a comment about it that might make it, that you might, that you have a question about? Or that do you think it's right for example. Do you think it's wrong? Uh, so A?

A: Yeah. Uh, well in that we have to know that when we are dividing by something that number is not 0 and so, well you have stated that, I mean it would be better to state it again. That we could divide by a in this situation, because a is not 0.

Mike: Okay, first of all you're talking to the wrong person. It was T who said this, I didn't say it. I wouldn't have ever said anything like that. So why are you looking at me?

A: Okay so before you say b+c divides a equals k + j you need to state once more that we can divide by a since a is not 0.

T: Well but then, that's just part of the actual theorem.

A: Right.

T: It says in the theorem itself, a can't be a divisor of b+c if a is 0 in the first place.

A: I mean that's the way I've learned, just write it down again as a given.
T: Just so.
Student: I don't agree with that.
B: I don't either. I think a better way to do that would be to just eliminate the line that's second from the bottom and say that k+j is the sum of two integers, which itself is an integer and then by definition you know that a is a divisor of it.
T: I agree.
Mike: Do you agree?
T: Yeah.
Mike: Okay, go ahead and take action then.
T: Okay.
Mike: Okay, right. Because then. So from this line, just because we're out of time, from this line what can you conclude?
(Some students answer quietly)
Mike: What does this say about a in relation to b+c?
(Some students answer quietly)
An.: That it is divisible by b+c.
Mike: That's right because that's the definition. So here, by definition this means, this line is equivalent to the definition of a divides b+c. Or you could write it out in English, a divides b+c. So this is a good proof, but the division part, if we've accepted the definition, this definition, then that's the definition that we want to refer back to. So that was a very good example. Thank you gentlemen. Thank you gentlemen. And so what we are going to do is start next time. I will ask people to present their proofs. Generally speaking we should be able to finish, oh, maybe about 6 proofs, 7 proofs in a day is typical. And what I want you to do is write up your, you're an-, your proofs, your personal proofs and turn them in before they are presented in class. So that's the standard written homework assignment is to write out your own personal theorem. You're not allowed to look at any textbook. You're not allowed to ask any other person who's not in this class about any of this uh, uh, Number Theory. You're not allowed to ask anybody else. It's all on you to do it yourself. You may ask me and uh, any questions you want and we'll set up office hours next time. I'm sorry we're late though. So, I'll just see you next time. On Friday. It's good to meet you and I'll look forward to seeing you on Friday.

Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $a|c$, then $a|(b-c)$.

PROOF: By definition $a|b$ means $\exists\, x \in \mathbb{Z}$ s.t. $ax = b$ and likewise $a|c$ means $\exists\, y \in \mathbb{Z}$ s.t. $ay = c$. So then $b-c = ax - ay$. By multiplicative distribution $b-c = a(x-y)$ which is also $b-c = a(x + {}^{-}y)$. Since $-y \in \mathbb{Z}$ then by addition of integers $(x + {}^{-}y) \in \mathbb{Z}$.

1.3

Let a, b, c be $\in \mathbb{Z}$. If $a|b$ and $a|c$ then $a|bc$.

<u>Pf</u>: By def. $a|b$ means $b = a\ell$ for some $\ell \in \mathbb{Z}$ and $a|c$ means $c = ak$ for some $k \in \mathbb{Z}$

Then $bc = a\ell \cdot ak$

$bc = a(\ell a k)$

$\ell a k \in \mathbb{Z}$ since $\ell, a, k \in \mathbb{Z}$

$\therefore a|bc$

(b)

Let $n = 10^k a_k + 10^{k-1} a_{k-1} + \ldots + a_0 = \sum_{n=0}^{k} 10^n a_n$

$m = a_k + a_{k-1} + \ldots + a_1 + a_0 = \sum_{n=0}^{k} a_n$

Proving $3|m \rightarrow 3|n$

if $3|n$ is true then the implication is true

So $3|n$ by def

$\Rightarrow 10^k a_k + 10^{k-1} a_{k-1} + \ldots + 10^0 a_0 = 3s$ where s is some int.

$\Rightarrow 10^k a_k + 10^{k-1} a_{k-1} + \ldots + 10^0 a_0 + (a_k - a_k) + (a_{k-1} - a_{k-1}) + \ldots + (a_0 - a_0) = 3s$

$\Rightarrow a_k(10^k - 1) + a_{k-1}(10^{k-1} - 1) + \ldots + a_0(10^0 - 1) + \underbrace{(a_k + a_{k-1} + \ldots + a_0)}_{m} = 3s$

Using proof 1.2 $\Rightarrow a|b$ and $a|c \Rightarrow a|b+c$

suppose, $b = a_k(10^k - 1) + a_{k-1}(10^{k-1} - 1) + \ldots + a_0(10^0 - 1)$

$c = m = a_k + a_{k-1} + \ldots + a_0)$

from 1.17

$3|(10^k - 1)(a_k + a_{k-1} + \ldots + a_0)$ is true

So for $3|b+c$, 3 must divide b and 3 must divide c. Since $3|b$ as shown above for $3|b+c$, 3 must divide c. Therefore if $3|m$ the $3|n$.

Mike: Okay, S are you ready. Okay why don't you go ahead and.

S: All right, the theorem that I am proving is given that a, b, and c are integers if b is divisible by a and c is divisible by a then b-c is also divisible by a.

Mike: Yeah and by the way, just as a matter of culture, usually it is phrased a divides b.

S: Oh, okay. A divides b.

Mike: It's the same thing, don't worry about it.

S: Oh, okay. Okay, so as we talked about on Wednesday by definition of b, uh a dividing b, then that means there exists x that is an integer such that $ax = b$ and likewise you can say the same if a divides into c that means there exists a y that is an integer such that $ay=c$. So then we can say that b-c is equal to $ax - ay$ by these uh. And um, by, since multiplication is distributive um, you can then say that b-c equals $a(x-y)$ which then you can rephrase as $a(x + -y)$ and since -y is also an integer and by addition of integers, $x + -y$ is also an integer which then shows that b-c can be divided by a, divisible by a.

Mike: Okay, do we have any comments or um questions for S? And for those people, who don't remember names, let's see you are T, T so you should introduce yourself as you speak. T.

T: What was your point of making it x plus -y.

S: Because we don't know anything about minus, really. We haven't talked about what exactly minus is.

T: Oh, I see, okay.

S: Um.

C: Hi, my name's C.

S: Hi.

C: Since we don't know anything about minuses, how do we know that -y is an integer?

S: Um. Well.

Mike: By the way, just to kind of, I mean I think I know about minus, you just subtract. I don't really worry about this kind of thing. Subtract two integers; you get an integer out of it. So let's, we're not approaching this topic from an axiomatic point of view, where we're given axioms for addition and so on. We know that if you subtract 2 integers you get an integer, we'll accept that. So leaving it just with x-y would be perfectly fine. Any other comment or question? Yes, Da.?

Da.: I think using theorem 1.1 you could make it a shorter proof.

S: Okay.

Mike: And how would you do that?

Da.: Um, if you just say that b and -c are integers and a divides $b + -c$ then that satisfies theorem 1.1 and that is the same as a divides b-c.

Mike: Okay. That's an alternative proof. By the way I would say that both those proofs are actually, Da.'s proof is not a shorter proof. It's an illusion to say it's shorter. Because you see he referred to another proof and the other proof entailed this, the steps that S presented here. So even though it appears shorter it's actually not conceptually a shorter proof so either one is fine. Either one of these are alternatives as we'll see in all of the theorems we'll see that there are alternative methods to proving. Any other comments or questions? Let me, thank you S, let me just say a couple of things about this that are particularly good. One, when S started she started by referring very specifically to the definition of what a symbol or a phrase meant and then used that definition in proceeding with the proof and that's what we were aiming for, to find that b-c satisfies the definition of divisibility. That a divides something means that a times something is equal to b-c. So that was a very good way, it was neatly written. Every sentence was a complete English sentence as opposed to just bullets. And so those are all good qualities of this proof. Okay. Any other comments on this?

--NEW CLIP--

V: So theorem 1.3 says that if we have integers a, b, and c then if a divides b and a divides c then a also divides bc. So by definition, just like she did, a divides b means that b is equal to a times some integer L and a divides c means that c equals a times some integer k. Then bc = $aL \cdot ak$ and we can factor out an a and then we see that Lak must be an integer since all three of these are integers to start with and then this statement here implies by definition of divides that a does divide bc.
Mike: Okay, what do people think? Think it's all right? L, does that sound good?
L: What?
Mike: Do you think it's correct?
L: Yeah, it's what I did.
(Class laughs)
Mike: That’s a good, I mean, that's a good affirmation. Looks good to me, that's what I did. That's one of the main reasons we think things are correct. It's what we believe. That’s great. Okay. Any comments on the style, the form, or anything about it?
K: You could put it in sentences. So like a minute ago you said she used complete English sentences, that's good. So I'm assuming that's a good thing.
(Class laughs)
Mike: Mm-hmm. Well but these are, for example this one is an English sentence. By definition a divides b, it's true that it uses the symbol, but it actually is an English sentence. By definition a divides b means b is equal to this for some known, there needs to be a period here, oh no, it carries on and there needs to be a period there.
(Class laughs)
Mike: Then bc equals, and if you, if you're just doing a sequence of where each one literally follows from the other then that's fine. So no, I would argue that this is a well constructed uh proof. Very good. Does anybody have any observations or comments about? Did you yourself V when you looked at this proof did you notice anything or think anything about it?
V: It's a little bit interesting that a would divide it twice, or a^2 would divide it.
Mike: Oh. Oh, so you mean to say you proved something more than you said.
V: I didn't prove that, I just noticed it and believe I could prove that.
Mike: Oh and what would you prove?
V: I would prove that a^2 divides bc.
Mike: Okay so why don't you write down what you, a better theorem. You have the same hypothesis and you get a better conclusion then that's a better theorem. Uh-huh, very good.
(Class laughs)
Mike: Yeah, so what you have done, what you have done is mathematics because you made an observation by having proved something you saw that indeed you had actually

observed that there, something more is true. And then write it down, record your observation you see because now you've proved a better theorem. So that's V's theorem.

(Class laughs)

Mike: a^2 divides bc. And you already have the proof. This is great you see, this is uh, and in fact one of the main things that you want to learn how to do throughout not only this class but elsewhere, is as soon as you've done something whether you've done a proof or you have an idea or you've somehow crystallized some notion that's the time to exploit it and to see oh, can I go further can I do something additional as you did right here. So this is a great example of that. Okay. Any other observations? Thank you V.

--NEW CLIP--

Mike: Okay, Ai., which direction are you going to prove?

Ai.: I think it's the same direction. Uh, so I am also proving that if 3 divides the sum of the numbers, the sum of the digits, then 3 divides the actual number as well. So what I'm starting with is if this, the implication is true, if 3 divides m then the whole implication holds true because the right side is true. So 3 divides n by definition is this sum of the numbers is equal to 3s. So if you break up this number and you do 10^k and this number plus you have $(a_k-a_k) + (a_k - a_k)$. So basically I am just trying to do some mathematical stuff here. And then I make this a_k10^{k-1} plus 10^{k-1}. I made this one summation and I made this one summation as $a_k + a_{k-1}$. So this number is m, the number which I stated above. So I have to basically prove that if this number is true then this number must be true for 3 to divide n. For that I used the proof of 1.2 that if a divides b and a divides c then a divides b + c. So supposing in this case that b is this whole number and c is this number, which is also equal to m as we've stated above. From the previous proof, which ..., we proved that 3 divides $10^{k-1}a_k$ plus, which is the same number as that. So, for 3 to divide b+c, which in this case is this whole number, 3 must divide b and 3 must divide c. So if 3 divides b, since we've proven it in 1.17 then for 3 to divide b+c, 3 must divide c. Therefore c divides, so if therefore if 3 divides c then 3 divides n.

Mike: Okay, how many of you followed that? How many of you uh, okay.

(Class laughs)

Mike: Okay, now, so you did not follow it? Is that what you're saying?

D: I got lost after like the second line.

Mike: Got lost. Yeah, yeah. I think, I think. By the way, so one great thing about this method of dealing with a class is reality. And you know those of us who are in the teaching biz know that if you start an argument and you start talking sort of fast and it has a lot of symbols in it that the audience is siesta time. It is essentially impossible to follow that kind of detailed argument. It really is. And you know that, right?

Ai.: Yeah.

Mike: Right. You couldn't follow that?

Ai.: Right.

(Class laughs)

Mike: So what we need to do is um, but math does have the property that you sometimes need to get in there and see well what does that sentence mean and really grip it.

B: After reading it I think I follow it now and I think you have, you might have some what of a problem. Because what you say is so for, so you know 3 divides b+c. Well that's your conclusion.

Mike: Yeah, so let's, I'll tell you what B, what I'd like to do is have people in order to really grapple with this, just right now talk to your neighbor. Okay? And look through this proof and really just try to, because it is completely written so there's no necessity for other explanation. And just start going through it, just start going through it line by line and just see what it means and every line and as soon as you get to a line you don't, you don't follow or you think is wrong you know then note it. So right now, start, talk to the person next to you. So your goal is your the, by the way, the way math papers are written, if you write a mathematical paper then it's sent out to a referee. So it's mailed out to somebody and then that person reads it and tries to figure out if it's actually correct. Okay? So you're now the referees of this thing. You're trying to read this and see is it really proving what he wants to prove and is every step logically following from the previous one. So go ahead tell, tell the person next to you. Right now, I want to hear noise. Okay?

Mike: Okay, so let's. Let me just ask for a couple of comments on this and then, and then we'll see if people, how, what you saw in this proof. Um, so why don't we begin with M. Did you have, did you and St., uh or I don't know who your group was. J, were you in that group?
J: I was, yeah.
Mike: Floater, a floater.
(Class laughs)
Mike: M, did you have a comment or a--?
M: Yeah I think for the last part, the 3 divides b+c, I think it's unnecessary that 3 divides b and 3 divides c also.
Mike: Okay, let me ask more globally, what is the theorem statement that he is proving?
K: If 3 divides m.
M: If 3 divides m and then 3 divides n.
Mike: Okay, what is he assuming and what is he trying to prove?
M: He's assuming that 3 divides m, right.
B: Oh wait.
Mike: Well which one is it?
B: In the beginning he says we want to prove 3 divides m means 3 divides n but then he assumes that, he assumes the conclusion and he says if I say the conclusion is true then the premise is true, but that's not what he wants to prove.
P: Oh, it's not a typo.
S: And it doesn't so much work to use 1.2 in this case considering the fact that the, going backwards, the converse of 1.2 isn't necessarily true. Like for instance if a=3, b=3, and c=1. b+c is not divisible by 3.
Mike: Okay.
Ai.: But this proof would work the other way because I assumed 3 divides n right? --
Mike: -- So the first fundamental difficulty with this proof, I would say, is that you just haven't stated what it is you are assuming and then starting from that assumption take steps to get to a conclusion. You see when I read this I wasn't clear whether the

assumption was that 3 divides evenly into the sum of the digits or whether the assumption was that 3 divides evenly into the total number. That wasn't clear to me. And as I read it, it didn't become clearer. I'm still not clear on which direction it is. A lot of steps, you see, are reversible because if it's something that's if and only if then you know you really can logically think of going both ways so it's not so much that it's wrong it's that it's not clear what the assumption is to start with and where you're headed. So to clarify things the very first thing you have to be 100% clear on is what it is you're assuming. So that's, that would be the first thing that you'd want to do is to make it completely clear what you're proving. So if this is what you're proving then that's what you should start talking about.

B: Since he was asked to do it 3 divides n implying 3 divides m and then he was asked to change it. Did you not change back what you have on your proof statement?

Ai.: Uh --

Mike: -- This was --

Ai.: --No, that's right.

Mike: This was changed back to the way he had it originally.

B: Because I'm just, I was going to say even if you had it to where it was 3 divides n implying 3 divides m, it still wouldn't work out the way you did it because you can't use 1.2 the way you did at the bottom.

Mike: Well, no, actually I think--

Ai.: You can pretty much use it, right?

B: No, because that's the, you're using the converse which isn't necessarily true.

Ai.: No what I'm doing is so if 3 divides b and 3 divides c right? So if 3 divides b is true, this is a 3, then 3 divides b+c. So if this is true already, right?

B: Right.

Ai.: So for this thing to be true, this whole thing, 3 must divide c, right. This must be true as well.

Mike: But you see the trouble is you assumed what you wanted to prove and then, and then assumed that this is also true, by the way. See so he assumed both directions and therefore, and then he concluded. See that's the problem. Okay, I'll tell you what ...Which are interesting and they're ideas when you're actually working on a proof and you're developing a proof often this is the kind of thing that you write down and you think about and I think it's sort of clever to take this number and add 0 in this form. You see how he did that? $a_k - a_k$, $a_{k-1} - a_{k-1}$, you know. He added 0 and then by using algebra, the distributive law, he could recognize it in this form. Well that's sort of a clever thing and maybe at, maybe that's at the heart of what you really want to use to make a proof. But in order, but an actual proof has to then take it and step logically from a clearly stated assumption to the proof. Okay? So why don't you go ahead and fix this up for next time, and then write a really neat proof of the other, let's do the other direction. That if 3 divides n then, that's what you assume. So the first thing you want to write down is that this number here is equal to 3s. So this is your assumption. But then what you want to prove is that 3 divides n implies 3 divides the sum of the digits. Okay? Okay, so we'll do that first thing next time.

Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$ does $a \mid \frac{b}{c}$?

$a \nmid \frac{b}{c}$ by counterexample

Let $a = 3$, $b = 12$, $c = 6$

$3 \mid \frac{12}{6} = 3 \mid 2$ which is false

1.21 Division Algorithm $m = nq + r$

We are given m and n as any integer that $m > n$. Therefore q would be an integer of $\frac{m}{n}$ and r would be the remainder from the division. For example $27 = 3 \cdot 7 + 6$. Then we can conclude $n \cdot q \leq m$ and $0 \leq r < n-1$.

Mike: So, um, tell me this, for most of you what are you thinking about right now?
(Al. begins to speak)
Mike: Al., what are you thinking about?
Al.: I'm thinking that's good, I didn't think of that at all.
(S says something; can't understand)
Mike: What's your name again?
W: W.
Mike: W. Yeah, W.
W: I was just thinking that's what I did in my head to check it for myself and then I tried to figure out how to prove it.
Mike: Okay, well I'll tell you what I'm thinking. I'm thinking I'm not quite clear exactly what we're doing. I'm not clear what the hypothesis is and what the conclusion is. It seems like I came in in the middle of a movie. That's my impression.
C: Okay.
Mike: You see because you started out a does not divide b minus c now, b divided by c, and I'm thinking okay wait where are we starting. Are we assuming something? If so, what are we assuming? Are we assuming that a divides b, a divides c? Are we back there? Are we thinking about somewhere in between, you know. I'm not oriented yet in exactly what we're doing so I'm a little bit confused about where we are. So what I would like to do, and by the way the fact that I'm a little confused I'm guessing that some of you are confused. Now maybe not. Is anybody confused about what sort of where we were, what we were assuming? No? Every single other person in this room is not confused.
D: I think it's because we, yeah, we have the proof in front of us and we read it before so when he just went up there and wrote the answer we just all followed. But if I walked into the room and had come in late and just sat down I wouldn't know what that was about.
Mike: You wouldn't know what that's about. Okay, so then for my sake, since you've got to deal with the slow kid in the class.
(Class laughs)
Mike: Tell me what's the hypothesis and what are you.
(C is writing on the board)
Mike: Okay, I see. So if a divides b and a divides c can we conclude that a divides b divided by c. Oh, okay. Okay, and then you're saying let a equal 3, b equal 12 and c equal 6. So then a divides b, yeah that's true. A divides c, that's true. But a does not divide b over c because 12 over 6 is 2 and 3 does not divide 2. So what do you conclude?
C: I'm concluding that for all, for all cases that you can't assume that a does not, a divides b over c.
Mike: Okay, did you hear what he said? Say it one more time.
C: Okay, I'm concluding that um, that for all cases that a does not necessarily divide b over c.
Mike: Okay. Now, now I want you to think very carefully about what you're saying because; I'll tell you what he said. He said I conclude that for all cases a does not necessarily divide b over c. That's what he said. Did you hear that? I conclude that for all cases a does not necessarily divide b over c. Is that what you meant to say?
C: Yes.

(Some laughter in class)
Mike: Sounds good to you?
C: Yes, sounds good to me.
Mike: I see, and that's why you said it.
(Laughter)
Mike: Okay, um. So let's think about what he said. I'll write it down.
(Mike writes what C said on the board)
Mike: Okay. That's okay. Now I'll give you a hint. This is really not right. I mean, I know what he's trying to say. It's just that what, if you actually read those words it doesn't actually say what it is he means. Yeah, T.
T: He could replace for all with there exists some. Cause if you have a equals 2, b equals 12, and c equals 6 then 2 divides into 12 divided by 6. However, but this case does not work. So there exist some cases that a does divide b divided by c, but not all of them.
Mike: Yeah. Okay, so okay, so let's just see. First of all, you know I know what you mean. I know what you mean. You're saying it's not the case, it's not necessarily true that if you have these hypothesis that a divides b over c. That's what you're trying to say. And so what you have is sort of a confusion of things. You're saying for all cases, a does not necessarily divide it. It's sort of a peculiar way to phrase it.
C: Okay, should I say there exists cases of a, b, and c where a does not divide b over c.
Mike: Correct, correct. And that's the same as saying so, so, I mean, there's sort of confusion here because you have for all and then it's not necessarily. You know, that's a little bit fuzzy. So what you really want to say is either given, if a divides b and a divides c then a does not necessarily divide b over c. That's a true statement. Or you could say it's not true that for all, all a, a divides b over c. But you don't want to say for all a. For example it would be wrong to say for all cases a does not divide b over c. That would be wrong because it's not true that for every single a, b, and c that a would not divide b over c. For some of them it would. Yeah, and what's your name again?
K: I'm K.
Mike: K.
K: What if you just moved for all cases to the end and phrased it a does not divide b over c for all cases.
Mike: Yeah, that's better. Yeah, that would be okay. But just, I guess what I'm, all I'm pointing out is when you're writing these things just think about what they mean. Just think about in English what it actually means and then you have. And quantifiers are very important, they, the for all and there exists and things. So this is great.
Mike: Are you ready?

--NEW CLIP--

Mike: Let's do 1.21, that's probably logically the next one which is the existence part. Who did that? All.?
All.: Well I just wrote down the Division Algorithm here. And I stated that we're given the m and n as any integer and that m is greater than n. Therefore um, we can conclude that q would be an integer of m divides by n and r would be the remainder from the division of m by n. Um, I did an example here and the next step is we can conclude that n times q will be less than or equal to m and r will be greater than or equal to 0 and less

than or equal to n minus 1. That's pretty much it.

Mike: Okay. Do you have any questions for All.?

K: Just one thing. I don't think it said anywhere that n has to be less than m. Because over here in 1.20 n is 45 and m is 33.

All.: That's right.

(All. erases m>n)

Mike: V.

V: How do you know it works for other numbers too?

B: I would just say that it's not any integer of cause I mean you could. Wouldn't it be the least integer such that you get the most? (Can't understand the rest)

Mike: What do you think? I mean, I'm trying to get a sense of the crowd here. I mean do you think that this is a good proof or not?

K: One thing I am just hesitant about is we're proving the division algorithm and he used m divided by n in the proof.

Mike: Uh-huh.

K: He used division in the proof so I don't know if that's okay.

Mike: An., what do you think?

An.: I don't know, I just, I've got a comment, I don't know what, how he got to his conclusion or anything. I'm just, it seemed kind of vague.

Mike: Mm-hmm. Yeah, S?

S: I'm not sure what it means to be an integer of m divided by n.

All.: Well uh, hmm. It will be like computer science, if you divide one integer by the other integer and you will get something like, maybe 4.6 and we take the 4 as the integer.

A: (can't understand) least integer.

S: Sorry, forget I said anything.

All.: (can't understand)

Mike: P?

P: Um, I was trying to do something similar, uh since you said computer science; I was using a computer science mindset too. I guess you're a CS major as well.

All.: Yeah.

P: All right. Because what I was thinking is when you get two integers and then use the division operation then you'll get a real number but if you take away everything after the decimal you'd be given the integer. That's what you were thinking as well.

All.: Exactly.

P: And you would just get the remainder by using that newfound integer and then subtracting it to get the remainder. Is that correct?

All.: Pretty much.

P: Can we use that? That would be cheating though.

Mike: I don't know, what do you think? I guess, I guess, first of all just to ground the discussion a little bit, I'm having trouble just with the very first line. Division Algorithm, m equals nq plus r. I'm not clear on what's the hypothesis, what's the conclusion?

All.: Um, I just wrote down the Division Algorithm right there (using his packet), at the top. It's just like the um, the theorem that we need to prove.

Mike: But what is it you're trying to prove? What's the hypothesis and what's the conclusion?

All.: The existence part of the division algorithm.

Mike: Right, that's what you're trying to prove but see maybe I should have written this out more completely because you abbreviated there. You just said Division Algorithm m equals nq plus r. But I guess I'm not clear on what the hypothesis is. What is the hypothesis? Suppose you were writing out the whole hypothesis and the whole conclusion of what your proof is trying to prove. What would be, what would be the whole hypothesis? Okay, so let me ask people, let me ask everybody here. So, um, so let me just ask somebody. I'm going to ask somebody right now, what is the hypothesis of the theorem he's trying to prove, okay? So let me pick somebody at random. So M can you tell me what the hypothesis is?

M: With two natural numbers m and n there exist some integers q and r such that $m = nq+r$.

Mike: Right, where r has that property.

M: Yeah.

Mike: So, right, so the point is that what you're trying to prove the hypothesis is right here. Let m and n be natural numbers then there exist integers q and r such that m equals nq plus r and r lies between 0 and n minus 1 inclusive. So that's, that's the statement that you're trying to prove. Okay? So one thing you want to try to avoid is abbreviations, particularly if abbreviations don't capture the essence of what it is you're trying to accomplish. So for example here we're given m and n as any integers. Is that really what you're given?

All.: Isn't written here, that m and n. (Pointing to his packet)

Mike: But see (Pointing to All.'s packet).

All.: Oh, okay.

Mike: Yeah, so these are natural numbers.

(All. corrects his proof)

Mike: All right. Okay, therefore q would be an integer of m over n. So what do you mean by that?

All.: What I said before, um, it will be the first digit. Let me give an example, um (he writes 27/3 = 7.)

Mike: I wonder if there's any way you could phrase it without using division. You know K brought up the problem, or maybe An., I can't remember who, brought up the question of using division. Was it you, yeah, brought up the question of using division which we may not have really; you know it's hard to know whether that's a well-defined term yet. Uh, maybe it's all right. Q would be an integer of. Of course that phrasing is not great but you explained what that meant. Could you do it in terms of multiples of n? Could you say something about what q is in terms of multiples of n? So you'd have 0 times n, and then n, and then 2 times n, 3 times n, 4 times n. What would be the q?

Ma.: (saying something I can't understand)

Mike: And what? Yeah, so you might want to, Ma. why don't you suggest it to All..

Ma.: So it's n times q is less than or equal to m and n times q is greater than m minus n.

Mike: N times q is greater than. N times q is less than or equal to m, less than or equal to, and then what's going to be bigger than m? N plus 1 times q. N times, no I'm sorry, n times q plus 1, I'm sorry.

All.: Is going to bigger than m?

A: No, n times q, the remainder is greater than 1 then n times q plus 1 is going to be less than.

(Several students are talking)

S: If you use the well-ordering axiom saying that q is the uh, greatest natural number such that n times q is less than m.

Mike: Or q plus 1 is the smallest one that's greater than is probably better.

K: No addition sign.

Mike: In other words this is just a way of saying that you, it's really saying the same thing that you're saying here; it's what this phrase might actually mean. That n times q is less than or equal to m but if you take an additional n then it becomes bigger than m. So q is the biggest number that you can multiply n by to stay less than or equal to m. Okay? So that's your q and then why is it that the r will be within range if you choose that q?

All.: That's what it says right here. That if n times q will be less or equal than m and if we plus 1 to the q and n will be in the range and r will be the remainder.

Mike: Okay, how would you, how would you manipulate that inequality that you have in order to demonstrate the size of r? R, by the way, is equal to m minus nq.

(Long pause while All. looks at the board)

Mike: Okay, um, so All., you just stare at it for a while. Let's uh, who did 1.22? Okay, Ma. why don't you go ahead and do 1.22 while he's thinking. You'll see it in just a second.

Difficult Proof

Mike: Um, does anybody have 3.15, that a polynomial has to have infinitely many, that is to say, um, for infinitely many integers that you plug into a polynomial you're going to get a composite number. Anybody have that? Okay, I'll tell you what then, why don't we work on that right now. Why don't we work on that right now because this is one, I think this is sort of a hard one and you know I don't know how to do it. But I think we can figure out how to do it if we work on it. So let's go ahead and see if we can talk about this one together. So this is 3.15. So let's make sure that everybody understands the situation. We have a polynomial that has integer coefficients. So we have f(x) and it's is an integer times x^n plus an integer times x^{n-1} and so on. And we have this polynomial and we're asking the question if you plug in integers for x, you plug in one thing of course you get an integer; you plug in something else you get an integer and so on. What this says is that for infinitely many of those you're going to have to get a composite number, you can't always get a prime. Now you might think you can always get a prime. Now look at the polynomial $x^2 + x + 41$. Let's do some arithmetic here. Okay? Let's just do some arithmetic. Here's your. What I'd like you to do. How many people have calculators? Does anybody have a calculator? I don't know if you need a calculator. But okay, so all those who have calculators, let's do the following thing. What I want you to do is tell me some number and I want you to plug it into the calculator, see what you get, and then determine whether or not it's prime. Can calculators do that? Some people have calculators that actually say check for primes. Anybody have a calculator like that? Say whether it's prime? Well then you'll have to check it in the old-fashioned way. Just divide by primes up to its square root. Okay? Okay, so here's what I would like you to do. So I'm going to ask one of you to say a number and then that number will be plugged into this and then it will be determined whether or not it's prime. So I'll just start asking people for numbers. So S, give me a number.
S: 42.
Mike: 42, okay. I want, I'm going to ask for 32 and let's see who's going to be the volunteer for 32? Back row of people? T and An. and Ch. will be. Plug in for 32 and determine whether or not it's prime. Okay? Go ahead and pick another number. So I'd like another number. W?
W: 25.
Mike: 25, okay. So let's go ahead and um, Ma., would you do 25? Plug it in, see what you get, and then determine whether or not it's prime. Okay, let's just go ahead and do a few others. Tr., do you have a number? Just pick a number, any number.
Tr.: 1,002.
Mike: No, no, no, that's way too big. We'll be here all day you see; it has to be a smaller number.
Tr.: 102.
Mike: Okay, I'll tell you what, let's pick --
(Class laughs)
Mike: -- 12, okay go ahead. Okay, 12, do 12, plug it in, determine whether or not it's a prime. Okay? I'm getting lots of good numbers here. Yeah, C?
C: 41.
Mike: 41, okay. 41, try 41. Okay, C, you can do that one without a calculator, okay. Okay, now somebody else? Somebody else want to? V?
V: 5.

Mike: 5. Try 5. So I'm putting these equal signs because people are going to tell me what the answer is and then we're going to say whether or not it's prime. Uh, yeah?
An.: 2.
Mike: An., 2. Okay, 2. F(2). By the way we could also choose negative numbers. Negative integers are okay.
K: Negative 0.
Mike: 0.
K: I said negative 0. You know in the newspaper when they have the weather, there's 0 and there's also negative 0.
Mike: No there isn't.
K: Yes there is.
Mike: Oh K.
K: At least in my home town there is.
Student: What?
K: I promise you this is true. There's like a measurement for 0 and negative 0 and I've never been able to figure out why.
V: You should call them.
S: Yeah ask them.
Mike: No, that means it's below zero, it's below zero.
K: Maybe so. It might have something to do with the ... required to.
Mike: No, I think it has more to do with your hometown.
(Class laughs)
Mike: Okay. Okay, so let's. Do we have any answers here? C? C, for 41 what do you have?
C: Do you want an exact number?
Mike: Yes, I do.
C: Okay, 1763.
Mike: 1763 and that's equal to what?
C: 43 times 41.
Mike: 43 times 41. Okay, so that number is not prime. This is a composite number, composite number. Okay? So that's a composite number. Now let's try some of these other ones. Has anybody finished? Yes, T?
T: It's 1097.
Mike: This is 32?
T: 32.
Mike: Okay, 1097. And is that prime.
T: Yeah, that's prime.
Mike: Prime. Okay, did anybody do 25? Uh, yeah, Ma.?
Ma.: It's uh 691.
Mike: 691.
Ma.: Prime.
Mike: Prime, prime, ooh. Okay, 12?
Tr.: 197.
Mike: What?
Tr.: 197.
Mike: 197.

Tr.: Prime.

Mike: Prime, prime, ooh. Okay, 5?

V: 71.

Mike: 71, 71.

V: Prime.

Mike: Prime. 2? 2?

Student: 47.

Mike: 4, 5, 6, 47. 47. 47, my college number, prime. And 0? 41, prime. And in fact, so this is just a sample, but in fact if you take any number, any integer at all from negative, well it says it on the notes here, from what negative 40 to 39 and you plug it into that polynomial. Every one of those is prime, like 80 in a row are prime. I mean it really is, I mean to me at least, this is sort of amazing. That you can have a polynomial, plug it in, get 40 in a row. And also if you think sort of inductively you know, and you get a little bit of experience and a thing comes out a certain way and then you guess. Well after you do like 80 in a row you might be tempted to guess that they're always going to be prime. So it really is a good cautionary tale about jumping to conclusions because here, even though we got 40 in a row we still can't guess that they're all prime. They're not all prime. Of course 41 is definitely not prime. The reason that you know C laughed when he suggested 41. C, why did you laugh?

C: Because I knew it was going to be composite.

Mike: Why?

C: Because it's 41 times 41 plus 41 plus 41.

Mike: Right. Every one of these terms, you see, is going to be divisible by 41. And therefore you know that when you plug in 41 you are definitely going to get a composite number. And in fact, by the way, remember what we're trying to do here. We're trying to aim for the question, why is it that for any polynomial whatsoever that there are infinitely many, number, infinitely many integers you can plug in to it that give you a composite number. That's what we're, that's what this was experimenting about. So that if you have any polynomial like this where the "a"s are integers, then there are infinitely many numbers you can plug in for x so that what you end up with is a composite number. So what I want you to do right this second is to tell me a case of this that you can definitely do. And maybe a case, that's, that by having this experience here, and this one, can you tell me a circumstance under which you know for sure there are infinitely many x that will give you a composite number. Don't tell me. Tell your neighbor right now, to uh, think about this. So if you're starting to think about this problem can you think of an instance in which you know for sure you can find infinitely many numbers x that will give you a composite number. That you can factor that.

(Students talking)

S: Or do they all have to be in that form?

Mike: Well, okay, no. 2x is an example of a polynomial where, in fact for 2x I guess for every single number except for 1 you're going to get a non-prime, you'll get an even number.

S: Yeah.

Mike: Right, right.

L: Take any number and multiply it by x and you're going to get the same thing.

Mike: Right. So anything like that. So if you just have a monomial, that's just one term, then it's true.
S: Right.
Mike: That's a good example. Can you think of other categories of polynomials that you can figure out? You know that's the way to do math, is that you look for opportunities, you look at cases you can actually do and then you try to expand them until they're all cases.

(Students talking)
Mike: Okay, I'll tell you what, let's uh, let's interrupt this for. Well no, I guess while you're doing this maybe we should try to get a few ideas from it and then let's go to the presentations. So, um, can anybody tell me a category of polynomials that you can in fact do? Yeah, C?
C: When you've got a_0 is 0.
Mike: When a_0 is 0. Very good. Okay. If you ever have a polynomial where this term is 0, why is it that you can find infinitely many values of x for which this polynomial is composite?
C: You're asking me?
Mike: Yeah, yeah.
C: All right, so um you can factor out an x out of all that.
Mike: Right.
C: And so now you've got x times some product, sum of integers.
Mike: Right.
C: And since they're both integers it's a composite number.
Mike: It's a composite number. Right. Exactly. So then we're in good shape and we've done a case where a, where the constant term is 0. And in fact when the constant term is zero, not only have you found infinitely many values of x for which it's true, but in fact all values of x, essentially are true. You can pick 2, or 3, or 4, or 5. I mean assuming that you have positive numbers; you're going to have composite numbers. Or even if you don't have positive numbers there will be composite number. They won't be natural numbers, but they'll be composite numbers. Okay, so, great. Okay? Now, so let me ask another group for another category of ones that you definitely can do. T, and An., and Ch., do you guys have another category?
An.: The category where x is divisible by a naught, a_0.
Mike: Where what is divisible by a_0?
An.: X, x divides into a_0.
Mike: Oh, oh, oh, oh. Okay, wait a minute, wait a minute. So let me see if I. So you’re saying we look at this polynomial and you're suggesting some values of x for which it is composite. Right? And what are those values?
An.: All where a_0 is divisible by x, or x divides a_0.
Mike: So what's what? Which divides what?
An.: X divides a_0.
Mike: Okay, now.
S: Other way.
An.: Or x is multiples of a_0.
Mike: Yeah. Well which is it.

(Class laughs)

An.: The last one.

Mike: I'm sorry, I shouldn't have said yes. I was assuming you'd be more assertive at that point. But go ahead, An., which one?

An.: X is a multiple of a_0.

Mike: Right, x is a multiple of a_0. Right. Because if x is a multiple of a_0, then for example suppose that x is equal to ka_0, then you could, what would this be equal to? I mean what could you factor out of it?

An.: You could factor out the a_0 then.

Mike: Right, because then $f(ka_0)$ would equal $a_n(ka_0)^n$ plus all the way down here it's ka_0 plus a_0 and so you'd have a_0s in every single term and it would factor out. Great. So for example this one right here. So tell me infinitely many values of x for which this will give you a composite number. Tell me a few of them.

An.: 41, 82.

Mike: Right.

An.: Whatever the next one is.

Mike: Whatever the next one is.

(Class laughs)

Mike: So 41, 82, I'll get my calculator.

(Class laughs)

Mike: 123, and so on. So this is all good. So there, this is an example you see that there are infinitely many. Okay, so have we proved the theorem?

C: Well almost.

Mike: Almost.

S: Taking into account that there are an infinite number of integers, there will be an infinite number of integers that will be divided, or can be divided by a_0.

Mike: That’s right, right. But have we, have we proved it yet?

Student: No.

Mike: Do you see any case that this doesn't cover?

J: One.

Mike: Yeah, J?

J: One.

Mike: One. How about a0 equal to 1? Ew. Yeah, okay, okay. So a_0 equal to 1 this method the trouble is oh jeez, yeah it's divisible by 1 but that's not quite good enough. But what we have done is focus attention. The only case we can't do, we've done every single case except for the case a_0 is equal to 1 or minus 1. That’s the only case we haven't done. So this is great because now we've focused our, we've seen what the real issue is. Or the remaining issue. The remaining issue now is when that final coefficient is 1. That’s the only thing we really can't do yet. So now we need to be clever, you know we need to figure, we need to think. Can anyone do that one? Did any group actually think about that one? Okay. We'll leave that one for next time because this is a really good challenging problem, but one you can do. It's, it really is, I think it would be, you get a lot of satisfaction from doing this theorem. Okay, so why don't we go ahead and start with R right now.

Difficult Proofs – Still don’t have a proof

Mike: We'll, what I'd like to do, you know in fact why don't we, let’s do these first and then we can work together on some of these if that's all right. Uh, because you know I think this idea that polynomials have composite numbers, infinitely many composites. This is one, a lot of these theorems I have a very clear, you know, I instantly remember how to do. This one I don't. This one is always a puzzle, I'm not sure I even know how to do this thing, you know?

T.A.: I was remembering from last year that was one. And I really want to see someone prove it for a_0 not being 1.

K: Yeah, I can say I have a solution for everything, I can do it for a_0 not being one or negative or one.

T.A.: I can do it for anything else but one. Yeah, one or negative one.

K: I can do it for anything when the absolute value of a_0 is not 1.

Mike: Mm-hmm.

T.A.: I really want to see it though.

Mike: Right.

T.A.: So you all have to figure it out.

Mike: Yeah, you really do have to figure it out. So, how in the world could we do that then?

S: I can think really straightforward on most things but I really I hit a wall basically. I went to office hours and we spent a long time thinking about it.

K: If one wasn't a funky number.

Mike: Yeah, it's not easy.

(Class laughs)

T.A.: Like if one times.

Mike: Yeah, one divides every number. Yeah. How can you, how can you. So in order for it to be a composite number you've got to figure out, you know, you some how have to know that it's uh, divisible by something less than the number itself, so. Hmm. In fact well, let's think about it. Okay. Let's see here. So D, tell me what the issue is, tell me what the problem is.

D: Well we're just trying to show that there are, that the polynomial will generate an infinite number of composite numbers on the integers as its input, I think, yeah.

Mike: Yeah, so all of the "a"s are integers and all of the um, I guess we should assume that this one is a positive integer just so that we get infinitely many. Well, I don't even know if that's necessary, by the way. So our goal is to show that if you plug in, so all of the “a”s are integers and you plug in a bunch of numbers x, integers x, and you need to know that for infinitely many of them you get a composite number. So in particular they can't all be prime, for example. They can't all give you primes, that whatever you plug in you get a prime. So lets' see. So what ideas, I mean how have you guys sort of tried to think about it? So okay, so let me, I'll tell you what I want you to do. I want you to tell me something that you actually can do. Um, about this. Um.

S: We already know that for a_0 is not equal to 1 then for every multiple, for every x that is a multiple of a_0, it is a composite number at least.

Mike: Yeah. Oh, by the way here is a very specific thing to do. Uh, you know, and that is to, one thing, sometimes it's useful and sometimes it's not, but one thing that we can actually do is take something that we actually can do about it, like you were just saying S, of saying that a_0, if a_0 is not equal to 1 then we can do it. One, minus one, then we know how to do it. And really try to understand it in as many different ways as we can with the hopes that somehow maybe the techniques that we, you know looking at it from some different way would help us prove the general case. So what is the technique for showing that um, if a_0 is equal to something other than one, how would you do it?

S: If a_0 divides x, then a_0 divides f(x).

Mike: So can you put that in modular arithmetic terms?

S: Um, if x is congruent to 0 mod a_0, then f(x) is congruent to f(0) mod a_0.

Mike: All right. If x is congruent to 0 mod a_0 then. Is it your birthday? Okay.

K: Oh, I was just going to say that then the reason I guess, the problem comes with a_0 being 1 then is everything is congruent to 0 mod 1.

Student: Right.

K: So, at a standstill.

Mike: Say it one more time, sorry.

K: This, we're going to come to a standstill because when a_0 is one, everything is congruent to 0 mod 1. So that's then our problem.

Mike: Mm-hmm.

S: Because I really, really like it can I explain where I hit my wall?

Mike: Okay, sure.

S: Basically I assumed that a_0 was equal to 1. Can I write?

Mike: Yeah, sure sure.

S: a_0 is equal to 1 so then we have f(x), one.

Mike: Right.

S: We know that all of this is going to be composite because you can divide out x for all these terms. So we have f(x) equals some composite number, we'll call this n, plus 1. And the wall was hit when we know that it could be the case that n+1 will be composite. n+1 it could also be prime and we just want to make sure that for all x we won't find an n+1 being prime. So, but I don't know what to do. So I just wanted to throw that out.

Mike: Mm-hmm. Well in fact I guess one thing that's clearer is if this number, if this number right here is--

K: --is odd.

Mike: -- odd.

K: Then it's a composite number.

S: Then it's composite.

Mike: Then you'd know. Well that's something.

S: But if it's even, then it's not so.

Mike: So if the, yeah, if it's always even. Well I'll tell you one thing; by the way, just looking at this this way is that you know this is an interesting way to phrase things. If you could, if we could find f(x) congruent to 0 mod something, you know for infinitely many xs. If we could find f(x) congruent to 0 mod something then we'd be in good shape right? Yeah, K?

K: Why would you say f(x) congruent to 0? Shouldn't it be f(x) is congruent to f(0)? Because the theorem we did said if a is congruent to b then f(a) is congruent to f(b). And then f(0) would be a_0.

Student: Which is congruent to--

K: So we'd have f(x). Oh, okay I got you. I understand.

Mike: Yeah, P?

P: I had a question. It was a confusion sort of. I was looking at theorem 3.11 and basically at the end if one is a_0 then I was thinking of a_0x^0 and anything raised to the 0 is 1 so that means that's basically a_0. I was confused because when you plug in 0 for x it would be 0 raised to the 0 and that's undefined. Well I plug it into a calculator and when I do, 0^0, on several calculators they say it's an error.

B: You don't need a 0, it's 0^1.

K: N is greater than 0.

P: Oh yeah, never mind. Okay.

Mike: Um, any ideas here, we've got to have ideas of how to approach this otherwise. How do you, what do you do when you are stuck? I guess this is the basic question. You know, here we're sort of stuck, how are we going to. In fact here is what I would like you to do right now while All. is still working here. Let's do the following. I want everybody to think of, since we can't think of the answer because we just somehow we haven't figured out how to actually do it. Instead of that, what action, what mental action are you going to take to get a new idea on how to approach this problem? So that is the question I am going to ask. I don't want to know what the answer is. First of all you don't know it; nobody in this room knows how to prove this. So that would be a silly question, because it's not there. But the question is what action are you going to take in order to get a new idea. Okay. What action, I mean what particular thing. I want you to feel that when you're stuck on something you can actually take specific action and move forward on it. So I want to know what are you going to do in order to take specific action, what specific action would, could you take to try to work on this problem. Okay. And just, you might say, well I don't know I would just stare at a piece of paper. That would be one possible answer. But let's see if we can think of answers that are more active than that. Okay? Tell your neighbor. Talk to your neighbor about it right now while All. is writing because I am going to go around and ask each person in the room what action will you, could you take that would get you moved forward. So you've all got to think of something.

Mike: Okay, so since it's sort of quieted down here let me, I presume that people have ideas. So let's go ahead and I'm going to just ask you to very quickly say what your, what a strategy would be. So D?

D: We were talking about something else, but beforehand.

P: Something else relevant to the class, to that problem.

D: I was thinking just step back and take a different approach. It's not very specific. But, like actively work towards looking for new perspectives on the problem.

Mike: And so what would you do, like in this case do you have any specific --

D: -- methods?

Mike: You know, or what would constitute in your mind a different approach? I mean what kind of thing can you think of?

D: Well one example would be, uh, earlier we observed that if n, we called it, was odd then it was trivial to show that f(x) is composite.

Mike: If which is odd?

D: The parenthesized. Everything but 1.

Mike: Oh yeah.

D: So that's kind of a different perspective, a different idea.

Mike: Uh-huh. If you look at, if that part of it had some sort of property, in this case if it were odd then you know, so maybe you could think of something other than odd that would somehow jog something. So part of it. So you could look at some part of it and see if some part of it was uh. Hmm. Okay, let's see. C, did you have some idea of how to approach?

C: I want to believe that it's true but I don't know that it's true. So I don't really think I can prove it until I can make myself feel that it's true in my heart. Like, so I guess I just look at it more until I feel that it's true.

Mike: You know this is very interesting that you say that, uh, you know that you believe in your heart before you can actually do it. It's interesting, I had a mentor here who is the reason I came to University of Texas, R.H. Bing he was a real famous topologist. And he claimed, I don't know if it's true or not because I think a lot of people do as you say they want to believe something. He claimed that when he was working on some problems, you know unsolved math problems, that he would work, well at least for this particular one, one really famous one. He said the way he would do it is he would work 2 hours to try to prove that it's true and then 2 hours to try to prove that it's not true and then 2 hours to try to prove that it's true and then 2 hours to prove, and so on. Because, and he claimed to not have any personal bias about whether or not something came out one way or another that he was just interested in knowing which it was. By the way, it is a terrific strategy to do that in the following way. Regardless of what your beliefs are about whether it's true or not. If you put your whole heart into trying to prove it is not true, then you will, you have to, what you have to face is you have to start saying well I need to construct a polynomial where everything I put in is going to be a prime, you know after a certain point. So can I, what coefficients can I put in that would cause that to happen or not cause you know by forcing yourself to actually try to make the opposite true you will see where the difficulty comes in trying to construct the opposite and then that can lead you to see what makes it true. Then you can say oh, I could never do that. See as soon as you can prove that you can never do the opposite, then that's a proof. That's the definition of a proof. So it's interesting that you bring that up, that you have to, you feel like you have to somehow get yourself to believe it. But, yeah I think it brought up an interesting idea at least in my head. I don't know if I conveyed it, but it really is sort of neat. Um, and then how do you go about trying to believe something is true? Well there are different ways to think about that. One is with some examples. You know you might just try to get more experience to get it. Ch., did you have any particular way to look at it? M, did you have a thought about how to?

M: No, I have the same idea with S. The last time we went to office hours we were thinking about the same stuff. We kind of have the same strategy.

Mike: Yeah, somehow it is interesting when you work on these things, and you just work and work and work, and one thing that you sometimes get a problem is you keep working in the same thing over and over again. You keep trying the same thing. So D's point of trying a new perspective is really important. You've got to think of some strategy that gets you off the dime, you know that really gets you moving. Yeah, K?

K: Maybe if you just made up a bunch of polynomials where a_0 is 1 and just observe when it was prime and when it was not prime you might notice a pattern there.

Mike: Yeah.

K: And it's probably a good strategy to try at least a million because we know that Gauss tried a million primes so following his example perhaps a million different.

Mike: Yeah, I think it wasn't a million primes. I think he factored all the numbers up beyond a million, I mean each number from up to a million, I'm not 100% sure.

K: Maybe we should try every number up to a million.

Mike: No, by the way I think that this is really an excellent, an excellent thing to do. Particularly those of you who knew computer stuff. I mean it'd be very simple to take some polynomials, you know random polynomials, with integer coefficients; have the computer write down which ones were prime and not prime and their prime factorizations. Or how about taking this polynomial that we have here. Here's a specific one, this one, $x^2 + x + 41$. Well of course that one we know because of 41 you know, we know by that that's always going to give you infinitely many composites

K: $x^2 + x + 41$.

Mike: Yeah. But no, but that's not such a great one because as you say we know the proof. Because if that, that's the one that if x is congruent to 0 mod 41, then f(x) is going to be congruent to 0 mod 41. So that we know that that's one. Yeah, P?

P: Maybe I am just exiting the freeway and taking another interstate, I got farther doing it, this is what I did. Since we know that if x is congruent to 0 mod a_0 or we're trying to prove x congruent to 0 mod a_0 then f(x) congruent to 0 mod a_0, that's the same thing as saying if a_0 divides x then a_0 divides f(x). And what I tried to prove, I got farther saying if f(x), if a_0 does not divide f(x) then a_0 does not divide x and I used proof by contraction to prove it.

Mike: Yeah, so that would be a way to get to this again. But um yeah, looking at the contrapositive it might be helpful. Saying, could you show what things don't divide the polynomial. Other ideas of how to think about it? Yeah, W?

W: We were just talking about um, looking back at the first chapter and seeing what we know abut relatively prime numbers.

Mike: Mm-hmm.

W: It seems like if you're calling all of the, like if we do it like S did, like you have the function and then you have n, so that those are relatively prime. And, uh.

Mike: Mm-hmm. Yeah if it's not true that these things give you infinitely many composite numbers, that means that all of them that it gives are prime after some point. It's the only other option. That all of them are prime. And after some point, you know for larger, certain x, from then on all of them are prime. Well, if they're all prime in particular they're all relatively prime to each other. Right, thinking about under what circumstances things are relatively prime. Thinking that the Euclidean Algorithm comes to mind or you know you can, you know ax +by =1. You could think about that. Yeah, C?

C: I just, I maybe had a breakthrough, maybe not. So I started factoring that, because basically to prove this we just have to show that everything but the plus 1, we have to show that that number is prime. That would be one way to prove this. So you factor it out and then you--

Mike: -- Now, wait wait, which is prime?

C: That the parentheses--

Mike: -- The whole thing is prime? F(x) is prime?

C: No, minus the 1.

Mike: Okay.

Difficult Proofs – Still don’t have a proof

C: So the stuff in the parentheses right now, so you factor out an x, and then you have to show that that's prime, and then I mean just keep telescoping it out. Well I don’t know.

Mike: Uh-huh, so.

C: It's just another idea.

Mike: Yeah, I wonder.

C: I don't know if it would work or not.

S: That's going to work for all x because then we're down to our previous condition and so then it would be for all x that are multiples of a1, a_1. Everything else, then that would be composite. Did that make sense?

Mike: Yeah, now by the way, by the way, in the direction of our intuition here I'm thinking about what fraction of numbers are prime. Would it be too frequent with this if every number you got was a prime? Would that be too many primes or not? I don't know. Okay, so let's see uh, other ideas? Other ideas on how to approach this? The unknown. Yeah, All.?

All.: I want to use that property but I have to know that n is a composite. Where if you know x^{n-1} is always divisible by x-1 if we know n is composite. But I don't know how to do it. And if you could break that down into just linear factors of x, instead of having, so then you only have some number times x plus a constant and do that for all the terms. And then you might get a linear function of x and then you can just show that since it's a linear function, I guess, they'll be composite numbers.

Mike: Hmm. Okay, okay, yeah I think this is great, you know figure out how do you think of new ideas. I don't know. Okay, let's uh.