CSC165 fall 2019

Mathematical expression:
more proof, modularity, prime characterization

Danny Heap
csc165-2019-09f@cs.toronto.edu
BA4270 (behind elevators)
Web page:
http://www.teach.cs.toronto.edu/~heap/165/F19/
416-978-5899

Using Course notes: Proof

(from DCS chair Marsha Chechik) Dear DCS Community!
I am very sorry to inform you that another tragic student death occurred in the Bahen Centre Friday night, September 27. The student WAS NOT registered in any Computer Science courses. Nevertheless, I know that this terrible loss will be felt by students, staff and faculty in our department. I understand that numerous members of the DCS community were in the building at the time of death and witnessed what occurred.
Round-the-clock support:

Feeling distressed? Find someone to talk to right now, and if there is an immediate risk, call 911.

Free 24/7 support is available outside the university. Students, staff and faculty can speak to a trained crisis worker at any hour of the day.

Good 2 Talk Student Helpline 1-866-925-5454. ProfessionAl counselling, information and referrals for mental health, addictions and well-being.

Gerstein Crisis Centre 416-929-5200

Distress Centres of Greater Toronto 416-408-HELP (4357)

The Centre for Addiction and Mental Health at 250 College Street

Anishnawbe Health Toronto Mental Health Crisis Line 416-360-0486

My SSP for U of T Students 1-844-451-9700. Immediate counselling support is available in 35 languages and ongoing support in 146 languages.

The following are some of the services available to students on all three campuses:

Downtown Toronto: Health and Wellness Centre (416-978-8030), located at Koffler Student Services

U of T Scarborough: Health & Wellness Centre 416-287-7065

U of T Mississauga: Health & Counselling Centre 905-828-5255

Outline

notes

linear combinations

$\forall a, b, c, p, q \in \mathbb{Z}, (a \mid b \wedge a \mid c \Rightarrow a \mid (bp + cq))$

prove $m, n \equiv 1 \bmod 3 \Rightarrow mn \equiv 1 \bmod 3$

converse of previous example?

$$m, n \in \mathbb{N}^+ \text{ and } m \mid n \Rightarrow m \leq n$$

proof pieces

A proof is a sequence of statements that flows left-to-right, top-to-bottom, each new statement justified by one or more of:

- given assumptions unpacked
- preceding statements
- external facts cited (if allowed)

The concluding statement should be what the proof claims.

useful pieces

We prove a powerful alternate definition of a number being prime using some external facts that are proven either in this week's worksheets or (last fact) not proven (yet)[1].

$$\forall x \in \mathbb{N},\ x \mid x \qquad \text{(Claim 1)}$$

$$\forall x, y \in \mathbb{N},\ y \geq 1 \wedge x \mid y \Rightarrow 1 \leq x \wedge x \leq y \qquad \text{(Claim 2)}$$

$$\forall n, p \in \mathbb{N},\ Prime(p) \wedge p \nmid n \Rightarrow \gcd(p, n) = 1 \qquad \text{(Claim 3)}$$

$$\forall n, m \in \mathbb{Z}^+,\ \gcd(n, m) \geq 1 \qquad \text{(Claim 4)}$$

$$\forall n, m, \in \mathbb{N},\ \forall r, s \in \mathbb{Z},\ \gcd(n, m) \mid (rn + sm) \qquad \text{(Claim 5)}$$

$$\forall n, m \in \mathbb{N},\ \exists r, s \in \mathbb{Z},\ rn + sm = \gcd(n, m) \qquad \text{(Claim 6)}$$

[1] See a step-by-step exercise proving this (question 2).

warmup

You showed in tutorial that if m and n are odd, so is mn. What is the translation of this into predicate logic? What is the corresponding claim for m and n not being divisible by 3? What about by 4? Which claims are true?

spoiler: primes are special

$$\forall n \in \mathbb{N}, (n > 1 \wedge (\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab)) \Leftrightarrow Prime(n)$$

prove converse...

$$\forall n \in \mathbb{N}, (n > 1 \wedge (\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab)) \Leftrightarrow Prime(n)$$

Notes