errata: csc16517f-errata@cs.toronto.edu

CSC165 fall 2017

Mathematical expression: modularity, prime characterization

Danny Heap
csc16517f@cs.toronto.edu
BA4270 (behind elevators)
Web page:
http://www.teach.cs.toronto.edu/~heap/165/F17/
416-978-5899

Using Course notes: Proof

Outline

notes

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.

Sometimes in the header we say where we're going

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) in problem set 2.

from last

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

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

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

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

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

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

divisors of p, n, find largest

$\gcd(4,6) = 2$ and $2 = -1\cdot 4 + 1\cdot 6$

$\gcd(5,7) = 1$

$3\cdot 5 - 2\cdot 7 = 1$

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?

$$\forall m, n \in \mathbb{Z},\ 2 \nmid m \wedge 2 \nmid n \Rightarrow 2 \nmid mn$$

$$\forall m, n \in \mathbb{Z},\ 3 \nmid m \wedge 3 \nmid n \Rightarrow 3 \nmid mn$$

$$\forall m, n \in \mathbb{Z},\ 4 \nmid m \wedge 4 \nmid n \Rightarrow 4 \nmid mn \quad \times$$

Counter-ex $m=2,\ n=6$

$m=2,\ n=2$

spoiler: primes are special

$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$

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

$\Rightarrow$ direction

contrapositive

$$\forall n \in \mathbb{N}, \underbrace{\neg Prime(n)}_{\sim} \Rightarrow n \leq 1 \vee (\exists a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \wedge n \mid ab)$$

$$n \leq 1 \vee (\exists d \in \mathbb{N}, d \mid n \wedge d \neq 1 \wedge d \neq n)$$

$\Rightarrow$

discussion: if we assume $\neg Prime(n)$ 2 cases

Case $n \leq 1$ | Case $n > 1$, so $d \mid n$ and $d \neq 1$, $d \neq n$

spoiler: primes are special

$\Rightarrow$ (by contra)

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

eg $\neg Prime(6)$ — $2 \mid 6$, so $\exists k$ st $2k = 6$ but $6 \nmid 2$

$6 \nmid 3$

since $d \mid n$, we know $\exists k \in \mathbb{Z}, dk = n$

let $a = d$, $b = k$ use Claim 2

$\Leftarrow$

prove converse...

$$\Longleftarrow$$

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

$$1 = gcd(a,n)$$

$$\Rightarrow 1 = s_1 a + t_1 n, \text{ some } s_1, t_1 \in \mathbb{Z}$$

$$1 = s_2 \cancel{a}\, b + t_2 n, \text{ some } s_2, t_2 \in \mathbb{Z}$$