ps1: FAQ @ piazza.
ps0: feedback on typing

t1: next Tues, same time, place: web page.

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

proof pieces

body

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 ✓ (probably in header)
- preceding statements – use ref. if necessary
- external facts cited (if allowed) – give a reference

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].

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

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

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

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

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

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

Bézouts lemma

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

warmup

$2k_1+1$ $2k_2+1$

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?

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

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

$\forall m, n \in \mathbb{Z},\ 5 \nmid m \wedge 5 \nmid n \Rightarrow 5 \nmid mn$

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

Prime numbers are atomic – cannot be split over a product!

spoiler: primes are special

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

Let $n \in \mathbb{N}$. assume $Prime(n)$.

Part 1 Prove $n > 1$.
Follows from definition $Prime(n)$

Part 2 Prove $\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab$

Let $a, b \in \mathbb{N}$. assume $n \nmid a \wedge n \nmid b$.

$\exists s_1, t_1 \in \mathbb{Z}, s_1 n + t_1 a = 1$ # worksheet
$\exists s_2, t_2 \in \mathbb{Z}, s_2 n + t_2 b = 1$ # 7, 2(a)

$s_1 s_2 n^2 + s_1 n t_2 b + s_2 n t_1 a + t_1 t_2 ab = 1$

$(s_1 s_2 n + s_1 t_2 b + s_2 t_1 a) n + t_1 t_2 ab = 1$

worksheet 7 2(b)

$n \nmid ab$

Part 1 $\wedge$ Part 2 ■

prove converse...

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

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

Let $n \in \mathbb{N}$. assume $\neg Prime(n)$, that is $n \leq 1 \vee \exists d \in \mathbb{N}, d \mid n \wedge d \neq 1 \wedge d \neq n$. WTS that $n \leq 1 \vee \exists a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \wedge n \mid ab$.

Case $n \leq 1$: Then first part of $\vee$ satisfied.

Case $n > 1$: $\exists d \in \mathbb{N}, d \mid n \wedge d \neq 1 \wedge d \neq n$. So $\exists k \in \mathbb{Z}, n = kd$. Let $a = d \wedge b = k$. WTS $n \nmid a \wedge n \nmid b \wedge n \mid ab$.

$n \nmid a \wedge n \nmid b \wedge n \mid ab$ # worksheet 7, 1.