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.

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.

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

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

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

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

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

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

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...

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

linear combinations

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

modular multiplication

$\forall a, b, c, d, n \in \mathbb{Z}, n \neq 0 \wedge a \equiv c \pmod{n} \wedge b \equiv d \pmod{m} \Rightarrow ab \equiv cd \pmod{n}$

Notes