errata in notes: csc165f17-errata@cs.toronto.edu

office hour:
MTW 4--5
I will
Lalla's
hours

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

Computer Science
UNIVERSITY OF TORONTO

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 derive, deduce
- external facts cited (if allowed)

The concluding statement should be what the proof claims.

sometimes headers suggest where you'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.

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

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

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

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

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

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

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

$\gcd(4,5) = 1 = -1 \cdot 4 + 1 \cdot 5$

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?

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

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

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

counterex $m = n = 2$ False

works for 5

Not for 6 ...

$\Leftrightarrow$ means $\Rightarrow \wedge \Leftarrow$

spoiler: primes are special

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

contrapositive

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

Prove $\Rightarrow$, assume, derive

$\forall n \in \mathbb{N}, \neg Prime(n) \Rightarrow \neg(\ldots)$

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

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

discussion $6 \nmid 2 \wedge 6 \nmid 3 \wedge 6 \mid 2 \cdot 3$

$8 \nmid 2 \wedge 8 \nmid 4 \wedge 8 \mid 2 \cdot 4$

a least in naturals

use the fact that can't divide bigger into smaller

prove converse...

Prove. $\cancel{\forall n}$

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

$\gcd(n,a) = 1$, then $1 = sa + tn$, for $s,t \in \mathbb{Z}$

e.g. $\gcd(5,8) = 1 = \cancel{-3 \cdot 15 + 2 \cdot 16}$ $-3 \cdot 5 + 2 \cdot 8$

Let $a,b \in \mathbb{N}$, $n \nmid a \land n \nmid b$

$1 = s_1 a + t_1 n$ since $\gcd(a,n) = 1$, Claim 6

$1 = s_2 b + t_2 n$ $\rightarrow$ into $s_3 ab + t_3 n = 1$?

linear combinations

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

<u>discuss</u> $b = k_1 a \wedge c = k_2 a$

$$bp + cq = pk_1 a + qk_2 a$$
$$= a(pk_1 + qk_2)$$

<u>Proof</u> Let $a, b, c, p, q \in \mathbb{Z}$. Assume $a|b \wedge a|c$. That is $\exists k_1, k_2 \in \mathbb{Z}, b = ak_1 \wedge c = ak_2$. Let k_1, k_2 be such values. Let $k_3 = pk_1 + qk_2$.

we show that $ak_3 = pb + qc$

Then $ak_3 = apk_1 + aqk_2$ # sub k_1 # k_2

$$= pak_1 + qak_2$$
$$= pb + qc \quad \blacksquare$$

modular multiplication

$n \mid a-c$, $n \mid b-d$ $\quad \mid ab-cd$

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

discuss know $n \mid (a-c)$

... try multiplying by b

$n \mid b(a-c) + c(b-d)$

$n \mid ba - bc + bc - cd = ab - cd$

$n \mid (ab - cd)$

modular multiplication

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

Let $a, b, c, d, n \in \mathbb{Z}$. Assume $n \neq 0$. Assume $a \equiv c \pmod{n} \land b \equiv d \pmod{n}$. We want to show $ab \equiv cd \pmod{n}$.

Then $a \equiv c \pmod{n} \Rightarrow n \mid (a-c)$

Similarly $n \mid (b-d)$

So $n \mid b(a-c) + c(b-d)$ # by linear combo

$n \mid ba - bc + cb - cd$

$n \mid (ab - cd)$ ∎

Notes

$$\left.\begin{array}{l} a_1 \equiv b_1 \\ a_2 \equiv b_2 \\ a_3 \equiv b_3 \\ \vdots \\ a_k \equiv b_k \end{array}\right\} \bmod n$$

$$a_1 \cdots a_k \equiv b_1 \cdots b_k$$
mod

$8 \cdot 8 \equiv 1 \cdot 1 \pmod 7$

RSA
public
key

$8 \equiv 1 \pmod 7$

$8 \times 8 \times \cdots \cdots 8 \equiv 1 \cdot 1 \cdots \cdots 1 \pmod 7$

$6 \cdot 6 \equiv 1 \pmod 7$

$6 \equiv 6 \pmod 7$

$6 \cdot 6 \cdot 6 \cdot 6 \equiv 1 \pmod 7$

$9 \equiv 2 \pmod 7$

$9^{100} \equiv ? \pmod 7$

$(9^3)^{33} \cdot 9 \equiv 8^{33} \cdot 9 \equiv 1^{33} \cdot 9 \pmod 7 \equiv 2 \pmod 7$