Constructive Logic (15-317), Fall 2021
Assignment 1: Say hi to logic!

Instructor: Karl Crary
TAs: Katherine Cordwell, Avery Cowan, Matias Scharager, Antian Wang

Due: Wednesday, September 8, 2021, 11:59 pm

Welcome to 15-317, Fall 2021 edition! In this homework assignment, you will practice some basic principles you'll need for the rest of the course. As a special exception to the usual rules, for this homework assignment, you may collaborate with other students in the class on the answers to all of the questions as long as you follow the whiteboard policy and do your write-up individually.

We require that you typeset your written solutions. Most students use LaTeX, but other software is acceptable. Please put each task on its own page to speed up grading.

The assignments in this course must be submitted electronically through Gradescope. Each assignment can have both a written and programming assignment. Weeks with both will split the assingment in two on Gradescope.

Links to the course's Gradescope can be found on Piazza. For this homework, submit two files: `hw1.pdf` (your written solutions), and `hw1.sml` (your natural deduction proofs).

One and one is one

Derive the following three judgments using the inference rules given in lecture (be sure to name each rule when you use it). Your solutions should go in `hw1.sml`. Compile your submission with `smlnj -m sources.cm`. This will check for syntax errors, but will not check for correctness[1]. There are examples of how to write natural deduction proof trees in the file `support/examples/nd_examples.sml`.

Task 1 (2 point).

$$(A \wedge (A \supset B)) \supset B \textit{ true}$$

Task 2 (3 points).

$$(A \wedge ((A \wedge A) \supset B)) \supset B \textit{ true}$$

Task 3 (3 points).

$$(A \wedge (A \supset B)) \supset (B \wedge B) \textit{ true}$$

Doing constructive mathematics

Definition. An integer a is said to *divide* an integer b, written $a \mid b$, if there exists an integer k such that $b = ak$. We write $a \nmid b$ for $\neg(a \mid b)$.

Task 4 (2 point). Give an (informal) constructive proof of the following proposition: for all integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Fun Fact. $2^{422687} \bmod 422687 \neq 2$

It's actually 376012.

Task 5 (3 point). Give an (informal) non-constructive proof of the following proposition: 422687 is composite. [2]

Task 6 (3 point). Give an (informal) constructive proof of the following proposition: 422687 is composite.

[1] On this assignment, gradescope will show feedback for tasks 1 and 2 as soon as you submit.

[2] Hint: Fermat has many cute little theorems, okay that was a lie he has just the one.

Task 7 (2 point)**.** Give an (informal) constructive proof of the following proposition: The number five is prime. Simply stating the definition of primality is not a full proof.[3]

Definition. The *Fundamental Theorem of Arithmetic* states that every integer greater than 1 either is prime or factors as the product of primes numbers, and moreover, that this factorisation is unique up to reordering of factors.

Task 8 (2 point)**.** Is the following proof that $3 \nmid 10$ constructive? Justify your answer.

> *Proof.* Assume to the contrary that $3 \mid 10$. Then there exists a k such that $10 = 3k$. By the fundamental theorem of arithmetic, k has some unique prime factorisation $k = \prod_{i=1}^{n} p_i$. So 10 factors into primes as $10 = 3 \prod_{i=1}^{n} p_i$. But we also know that 10 factors into primes as $10 = 2 \times 5$. The existence of two distinct prime factorisations for 10 contradicts the uniqueness guaranteed by the fundamental theorem of arithmetic. We thus conclude that $3 \nmid 10$.

[3]Our solution is a few sentences.