Discrete Math: Introduction 9/14

Instructor: Antonio Khalil Moretti
amoretti@cs.columbia.edu

➔ Better to post on piazza than to email me.
~150 students, unable to respond to emails

8 TA's (see CourseWorks for Office Hours)

Grading: HWs (~6) 45%, Exams (~3) 45%, participation 10%
(help record lectures or scribe notes)

(Tentative sketch of topics)

Outline:

Part I — Numbers, Sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, Functions, Quantifiers, Logical Statements, Proofs & Proof Techniques, Proof by Induction, Contradiction, Contrapositive, Direct, Bijections, Cardinality, Fundamental Thm of Arithmetic

Part II — Properties of Numbers, Binomial Coefficients, Binomial Thm, Permutations, Divisibility, Factors & Factorization, Euclid's Algorithm, Polynomials, Modular Arithmetic, Relations, Congruence, Groups, Fermat's Little Thm, Pythagorean Triples

Part III — Probability, Conditional, Marginal, PMFs, Random Variables, Expectation, Variance, Generating Functions, principles of Combinatorics, Recurrence Relations, Graphs, Trees, Advanced Topics

Def A proposition is a declarative statement that is True or False

Ex This course has three exams

We can use variables to denote propositions and negate them.

Def A proof is a verification of a proposition by a chain of logical deductions

A theorem is a proposition that has been proven.

Lets take a look at some simple proof techniques and examples

Def A rational number $q \in \mathbb{Q}$ is one that can be expressed as the ratio of two integers $a, b \in \mathbb{Z}$ such that $q = \frac{a}{b}$ where a, b are coprime (their $GCD(a,b) = 1$)

Thm $\sqrt{2}$ is irrational

Proof: We'll use the idea that a proposition cannot simultaneously be true and false

We will assume the proposition $(\sqrt{2} \notin \mathbb{Q})$ is false (i.e. $\sqrt{2} \in \mathbb{Q}$) and then derive what we can to see if we find something incorrect. Since nothing false can come from something true, if we reach a falsehood we will know that our original assumption was incorrect.

This is called proof by contradiction.

Lets assume $\sqrt{2}$ is rational. Then it can be expressed as a ratio of two coprime integers a, b

$\sqrt{2} = \frac{a}{b}$, Squaring both sides, $2 = \frac{a^2}{b^2}$ we find $2b^2 = a^2$

Since $2b^2 = a^2$, or $a^2 = 2b^2$, we know that a^2 is even.

$\Rightarrow$ Q: Do we know that a is even?

I want to prove the following Lemma or Corollary

if a^2 is even then a is even

A digression on logic

Let p, q be propositions. We can form a truth table by treating propositions as functions with boolean values along w/ operations of negation, and, or

p	q	$\neg p$	$p \wedge q$	$p \vee q$
T	T	F	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	F

Def

We define the implication $p \Rightarrow q$ for the proposition ("p implies q") or "if p, then q" which is a function of p and q

We define the biconditional $p \Leftrightarrow q$ or "p if and only if q" as follows

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

p is called the hypothesis
q is called the conclusion

To form the contrapositive, swap and negate the propositions. ($\neg q \Rightarrow \neg p$)

Can check from truth table that contrapositive is equivalent to $p \Rightarrow q$

p	$\neg p$	$\neg q$	q	$\neg q \Rightarrow \neg p$	$p \Rightarrow q$
T	F	F	T	T	T
T	F	T	F	F	F
F	T	F	T	T	T
F	T	T	F	T	T

Def proof by contrapositive

Ex if n^2 even then n even

Remark: A statement and its contrapositive are logically equivalent

To prove this, can use contrapositive "if n odd then n^2 odd"

$n = 2m+1$

$n^2 = (2m+1)(2m+1) = 4m^2 + 4m + 1 = 2\underbrace{(2m^2+2m)}+1$

$= 2r+1$ which is odd by def.

Therefore if n is odd, then n^2 odd, and equivalently, if n^2 even then n even.

Back to our proof $\Rightarrow$ We know that $a^2 = 2b^2$ is even and thus a is even

Since a is even it can be written as $2k$ for $k \in \mathbb{Z}$

Therefore $2b^2 = (2k)^2$

$2b^2 = 4k^2$

$= 2(2k^2)$, or $b^2 = 2k^2$, so b^2 is even.

We know from our corollary that if b^2 is even then b is even

$\Rightarrow$ So a is even, and b is even

By definition the $GCD(a,b) \neq 1$

However this is a contradiction, we assumed that $\sqrt{2}$ was rational and thus a,b were coprime. Therefore $\sqrt{2}$ cannot be expressed as $\frac{a^2}{b^2}$ for coprime $a,b \in \mathbb{Z}$. $\square$

Lets look at another proof by contradiction.

Def (prime)

A natural number $n \in \mathbb{N}$ is prime if $n > 1$ and n cannot be written as a product of smaller numbers. That is n has no positive integer divisors other than 1 and n.

Thm (Fundamental Thm of Arithmetic)

Every positive integer n has a prime factorization which is unique except for the reordering of the factors

$$n = \prod_{i=1}^{k} p_i^{e_i}$$

We will prove this later in the course using strong induction to show ~~uniqueness / and~~ existence and Euclids Lemma to show uniqueness.

Thm if p is prime, then $\sqrt{p}$ is irrational.

Proof (by Contradiction)

Write $\sqrt{p} = \frac{a}{b}$ for $a,b \in \mathbb{Z}$ with $GCD(a,b) = 1$

Then $p = \frac{a^2}{b^2}$ and $a^2 = pb^2$

By the Fundamental Thm of Arithmetic

b^2 can be written via prime factorization so that

$\cancel{b^2 = q_1^{2m_1} q_2^{2m_2} \cdots q_r^{2m_r}}$ $b^2 = (p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k})^2$

Lets spell this out explicitly

Take a number 120 and write its prime factorization

Ex $120 = 2^3 \cdot 3^1 \cdot 5$

By the law of exponents, when we square a number, the exponents in the prime factorization get multiplied by 2 and are thus even

Ex $(120)^2 = (2^3 \cdot 3^1 \cdot 5)^2 = 2^6 \cdot 3^2 \cdot 5^2$

This means that b^2 can be written as follows

$$b^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k}$$

Looking at the original expression $a^2 = pb^2$ we have

$$(q_1^{2m_1} q_2^{2m_2} q_3^{2m_3} \cdots q_r^{2m_r}) = p \cdot (p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k})$$

We will consider two possible scenarios. This is called proof by cases.

1) prime number p occurs in the unique factorization of b^2

i.e. p is one of the $p_1 \cdots p_k$'s.

if this is the case, we have $p \cdot p^{2n} = p^{2n+1}$ and thus p has an odd power. This is a contradiction, because by definition, the exponent must be even.

2) prime number p is not included in the prime factorization of b^2

if this is the case, then p has a power of 1 and again, p has an odd power. This is a contradiction again b/c by definition, the exponent must be even due to the equality with the left hand side. $\square$