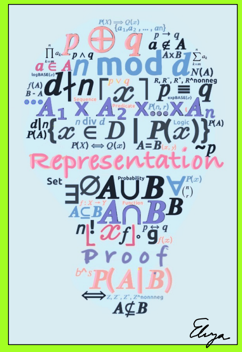
Discrete Structures



Lecture 9: Numbers and sequences

Susan L. Epstein
HUNTER

1

Last time

★ **More concepts support more proofs**

- How to do proofs by cases, contradiction, contraposition
- The parity property
- The triangle property
- How to prove with floors, ceilings, primes

Fall 2023 CSCI 150 2/29

2

Today's outline

- Classical theorems in number theory
- Sequences
- Summations and products

Real datasets often have exploitable patterns

3

Conjectures and theorems

Conjecture = claim that a statement is true

1637: Pierre de Fermat conjectured For $n > 2,\ \nexists\ a, b, c \in \boldsymbol{Z}^+\ a^n + b^n = c^n$

1986: Kenneth Ribet showed that if the Taniyama–Shimura conjecture were correct, then Fermat's theorem would be true

1993: Andrew Wiles presented a proof of Taniyama–Shimura (took 7years)
But just before publication, Wiles found an unjustified statement!

1994: Wiles revised the proof, it was checked by others and published.

1742: Christian Goldbach conjectured
$\forall x \in \boldsymbol{Z}^+, (x > 2)\ \exists$ primes $a, b \ni x = a + b$

2013: T. Oliveira e Silva verified by computer this true for $x < 4 \cdot 10^{18}$ but still an open problem

18th century: Euler conjectured $\nexists a, b, c, d \in \boldsymbol{Z}^+ \ni a^4 + b^4 + c^4 = d^4$

1987: Noam Elkies proved it wrong and Roger Frye used a a computer to find a counterexample: $95{,}800^4 + 217{,}519^4 + 414{,}560^4 = 422{,}481^4$

4

Proof by contradiction skeleton

Theorem: (copy the statement here)

Proof:

Assume: the negation of the conclusion

be general: any state any assumptions

We will show that this assumption logically leads to a contradiction.

Clarify your logic with a reason for every assertion
Display equations and inequalities clearly

Contradiction. Because the assumption led to a contradiction, negation of the assumption.

QED

$\sqrt{2}$ is irrational

Theorem: $\sqrt{2}$ is irrational.

Proof:

Assume: $\sqrt{2}$ is rational.

We will show that this assumption logically leads to a contradiction.

By definition of rational, if $\sqrt{2}$ is rational, then there are $p, q \in \boldsymbol{N}, q \neq 0$ with no common factor such that $\sqrt{2} = \frac{p}{q}$.

Then $2 = \frac{p^2}{q^2}$, so $2q^2 = p^2$, and by definition of even p^2 is even and (by slides 23 and 25 in Lecture 8) p is even.

By definition of even, for some $k \in \boldsymbol{N}, p = 2k$ and $p^2 = 4k^2$, so $2q^2 = 4k^2$.

Then $q^2 = 2k^2$ and q^2 and q are also even.

Thus p and q have 2 as a common factor. Contradiction.

Because the assumption led to a contradiction, $\sqrt{2}$ is irrational.

QED

Lemma 1 (for the next theorem)

Theorem: For any integer a and any prime number p, if $p|a$ then $p \nmid (a+1)$.

Proof:

Let a be any integer and p be a prime such that $p|a$.

Assume: $p|(a+1)$. By definition of |, there is some integer k such that $pk = a + 1$.

We will show that this assumption logically leads to a contradiction.

Because p is prime, $p > 1$.

But since $p|a$, by definition of |, there is some integer b such that $pb = a$.

Hence $pk - pb = a + 1 - a = 1$ but also $pk - pb = p(k - b)$ so $p(k - b) = 1$.

Since $\boldsymbol{Z}$ is closed under multiplication and subtraction, $p > 1$,and the only divisors of 1 are 1 and -1 (proved on slide 4, Lecture 7), $p = 1$ and is not prime.

Contradiction. Because the assumption led to a contradiction, $p \nmid (a+1)$..

QED

Fall 2023 CSCI 150 7/29

7

Proof by cases skeleton

Theorem: If A_1 or A_2 or… or A_n then C.

Proof:

Let/Assume/Suppose: Name variables and state what they stand for
be general: any state any assumptions

We must show that C is true in each of the following cases:

Case 1: If A_1 then C.

Case 2: If A_2 then C.

…

Case n: If A_n then C

Clarify your logic with a reason for every assertion
Display equations and inequalities clearly

Thus C is true regardless of which is the case.

QED

Fall 2023 CSCI 150 8/29

8

Lemma 2 (for the next theorem)

Theorem: Any integer $n > 1$ is divisible by some prime p.

Proof:

Let n be any integer. Then either n is prime or n is not prime.

We must show $n > 1$ is divisible by some prime p is true in both cases.

Case 1: n is prime. Since $n \bmod n = 0, n$ is divisible by a prime, itself.

Case 2: n is not prime. Then n has a standard factored form

$$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$$

where p_1 is a prime and n is divisible by p_1.

Thus n is divisible by some prime p is true regardless of which is the case.

QED

Proof skeleton

Theorem: (copy the statement here)

Proof:

Let/Assume/Suppose: Name variables and state what they stand for

be general: any state any assumptions

We must show that…

multiple grammatically correct sentences

Clarify your logic with a reason for every assertion Thus Then

Therefore So Hence Consequently It follows that

By definition of By substitution Because Since

Display equations and inequalities clearly

QED

There are infinitely many primes

T19 (in Appendix A): If $a < b$, then $a + c < b + c$.

Theorem: The set of all primes is infinite.

Proof:

Assume: there are finitely many primes.

We will show that this assumption logically leads to a contradiction.

Let p be the largest prime and let P be the product of all primes up to and including p, that is, $P = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p)$

Clearly $P > 1$ so by Lemma 2 some prime divides P.

Let q be such a prime divisor of P.

Then, by Lemma 1, $q \nmid (P + 1)$.

Because $0 < 1$, by T19 $P < P + 1$.

By definition of prime, $P + 1$ is prime, but $P + 1 > \mathrm{P} > \mathrm{p}$. Contradiction.

Because the assumption led to a contradiction, there are infinitely many primes.

QED

Fall 2023 CSCI 150 11/29

11

Today's outline

- ✓ Classical theorems in number theory
- Sequences
- Summations and products

Fall 2023 CSCI 150 12/29

12

Review: relations

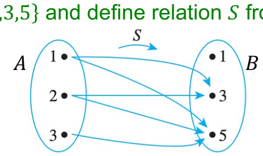
- Binary relation R from set A to set B is a subset of their Cartesian product $A \times B$

If $A = \{1,2,3\}$ and $B = \{1,3,5\}$,
$A \times B = \{(1,1), (1,3), (1,5), (2,1), (2,3), (2,5,)(3,1), (3,3), (3,5)\}$
$R = \{(1,3), (1,5), (2,3), (2,5), (3,5)\}$ is a relation that collects the pairs
$\{(a,b) | a \in A, b \in B, a < b\}$

- Set A is the domain of R and set B is the co-domain of R
- For $(x, y) \in A \times B$ and R a relation from A to B, x is related to y by R (written xRy) iff $(x, y) \in R$

- Can picture a relation with an arrow diagram

$A = \{1,2,3\}, B = \{1,3,5\}$ and define relation S from A to B to mean $x < y$



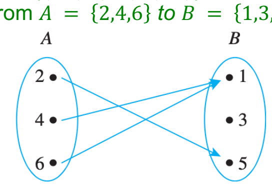
13

Review: functions

Binary function F from set A to set B is a relation with domain A and co-domain B where for every $a \in A$ there is exactly one $b \in B$ such that $(a, b) \in F$

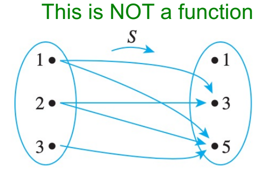
- If $(a, b) \in F$ and $(a, c) \in F$ then $b = c$
- If $(a, b) \in F$, then b is written $F(a)$ and read "F of a"

$F = \{(2,5), (4,1), (6,1)\}$ is a function from $A = \{2,4,6\}$ *to* $B = \{1,3,5\}$



Domain = ?
Co-domain = ?

This is NOT a function



14

Motivation

- A major goal of mathematics is to discover and characterize patterns in the world, particularly those that repeat
- Sequences are the principal mathematical structure with which to study such patterns
- Sequences represent patterns in some order…and such order allows us to represent and process infinite sets, both theoretically and on a machine with finite memory in finite time

15

Sequences

- Sequence = function whose domain is a subset of $\boldsymbol{N}$ and whose co-domain is the elements the function generates
  - a_i is the ith term in the sequence and i is its index
  - Repetition is allowed (g,o,o,d)
  - Order matters (g,o,o,d) ≠ (d,o,g,o)

Note that sequences are enclosed in parentheses

- Domain of a finite sequence $(a_m, a_{m+1}, \ldots, a_n)$ is all integers $\{m, m+1, \ldots, n\}$ between 2 values $m, n \in \boldsymbol{Z}, m \le n$
  $(0,1,2,3,4,5)$ $(15,16,17)$
- Domain of an infinite sequence $(a_i, a_{i+1}, \ldots)$ is all integers $\{i, i+1, \ldots\} \ge i$ for some $i \in \boldsymbol{N}$
  $(3,4,5, \ldots)$ $(25,26,27, \ldots)$
- An infinite sequence can have a finite co-domain

  $a_j = j \bmod 3$ ∀ integers $j \ge 0$ is $(0, 1, 2, 0, 1, 2, \ldots.)$ with co-domain $\{0,1,2\}$

16

Formulas for sequences

- Formula for a sequence = rule to produces term a_i for any i in its domain
  domain: $\{0,1,2,3,4,5\}$ rule: $a_i = (-1)^2, i \geq 0$, sequence: $(1,-1,1,-1,1,-1)$
  domain: $i \in \boldsymbol{N}, i \geq 2$ rule: $a_i = i^2 + i + 3, i \geq 2$, sequence: $(9,15,23,\ldots)$
- Alternating sequence has a single value in all its even positions and a single value in all its odd positions

  $c_j = (-1)^{j+1}3$ $\forall$ integers $j \geq 2$ defines $(-3,3,-3,3,\ldots)$
- Arithmetic sequence $(a, a+b, a+2b, \ldots)$ has formula
  $a_k = a + (k-1)b$ for $k \in \boldsymbol{N}, k \geq 1$
  $a = 4, b = 3 \quad (4,7,10,13,\ldots)$ $\qquad a = 7, b = 2 \quad (7,9,11,13,\ldots)$
- Geometric sequence $(a, ar, ar^2, \ldots)$ has formula $a_k = ar^k$ for $k \in \boldsymbol{N}, \boldsymbol{k} \geq 0$
  $a = 4, r = 3 \quad (4,12,36,108,\ldots)$ $\qquad a = 3, r = 2 \quad (3,6,12,24,\ldots)$
- Can change the term name, change the index name, and start at a different value but still produce the same sequence

  $a_k = \frac{k+1}{k-2}$ $\forall$ integers $k \geq 3$ begins with $\frac{4}{1}, \frac{5}{2}, \frac{6}{3}, \ldots$

  $b_i = \frac{i-1}{i-4}$ $\forall$ integers $i \geq 5$ begins with $\frac{4}{1}, \frac{5}{2}, \frac{6}{3}, \ldots$

Fall 2023 CSCI 150 17/29

17

To find a formula, look for a pattern

$$\left(\frac{1}{n}, \frac{2}{n+1}, \frac{3}{n+2}, \ldots, \frac{n+1}{2n}\right)$$

Numerator starts at 1 and increases by 1
Denominator starts at n and increases by 1

$$a_k = \frac{k}{n+k-1} \ \forall \text{ integers } 1 \leq k \leq n+1$$

Or index from 0: $a_k = \frac{k+1}{n+k}$ $\forall$ integers $0 \leq k \leq n$

$$\left(1, -\frac{1}{8}, \frac{1}{27}, -\frac{1}{64}, \ldots\right)$$

Denominators is clearly cubes: $1^3, 2^3, 3^3, 4^3, \ldots$
Alternating signs $+,-+,-,+,-,\ldots$ achieved with $(-1)^{k+1}$

$$a_k = \frac{(-1)^{k+1}}{k^3} \ \forall \text{ integers } k \geq 1$$

Or index from 0: $a_k = \frac{(-1)^k}{(k+1)^3}$ $\forall$ integers $j \geq 0$

Fall 2023 CSCI 150 18/29

18

Today's outline

- ✓ Classical theorems in number theory
- ✓ Sequences
- Summations and products

Review: intervals

- $\boldsymbol{R} = (-\infty, \infty)$
- Interval = single contiguous subset of $\boldsymbol{R}$
- Closed interval $[x, y]$
- Open intervals
  - (x, y)
  - (x, ∞)
  - $(-\infty, x)$
- Half-closed intervals
  - $[x, y)$
  - $(x, y]$
  - $[x, \infty)$
  - $(-\infty, x]$

$3 \in (-1,4)$

$4 \notin (-1,4)$

$4 \in [-1, \infty)$

Summation with Σ

- How many integers are there in

  $[2,7]$? $[3,4]$? $[0,100]$? $[m,n]$?

  How many elements are there in $\left(\frac{1}{n}, \frac{2}{n+1}, \frac{3}{n+2}, \ldots, \frac{n+1}{2n}\right)$?

- Series $\sum_{k=m}^{n} a_k$ is the sum $a_m + a_{m+1} + \cdots + a_n$ of the $n - m + 1$ terms of the sequence $(a_m, a_{m+1}, \ldots, a_n)$ from its lower limit $k = m$ to its upper limit $k = n$

For sequence $a_k = k^3$ ∀ integers $k \geq 2$, sum of the first 5 terms is denoted

$$\sum_{k=2}^{6} k^3 = 2^3 + 3^3 + 4^3 + 5^3 + 6^3$$ Leave it this way

If you really care about what number results, use a computer.
What CSCI cares about is your thought process

More on series

- Index of summation for a series can also be a set

  $\sum_{x \in \{1,6,8\}} (x^2+1) = (1^2+1) + (6^2+1) + (8^2+1)$

- Typically a series is generated by a pattern

For sequence $a_k = \frac{(-1)^i}{i+3}$ ∀ integers $k \geq 0$, sum of first $n+2$ terms is denoted

$$\sum_{i=0}^{n+1} \frac{(-1)^i}{i+3} = \frac{(-1)^0}{0+3} + \frac{(-1)^1}{1+3} + \frac{(-1)^2}{2+3} + \ldots + \frac{(-1)^{n+1}}{n+1+3} =$$

$$\frac{1}{3} + \frac{-1}{4} + \frac{1}{5} + \cdots + \frac{(-1)^{n+1}}{n+4}$$

Manipulating summations

$$\sum_{i=1}^{n+1} \frac{1}{i^3}$$

- Separate off the first term:

$$\frac{1}{1^3} + \sum_{i=2}^{n+1} \frac{1}{i^3}$$

- Separate off the last term

$$\sum_{i=1}^{n} \frac{1}{i^3} + \frac{1}{(n+1)^3}$$

- Rewrite as a single summation

$$\left(\sum_{j=0}^{n} 5^j\right) + 5^{n+1} = \sum_{k=0}^{n+1} 5^k$$

Fall 2023 CSCI 150 23/29

23

Index is a dummy variable

- Dummy variable derives its meaning from its local context

$$\sum_{k=1}^{3} k^6 = \sum_{t=1}^{3} t^6$$

- Using previous slide's manipulations may require change of a variable

$$\sum_{k=0}^{6} \frac{1}{k+1}$$

Change to $j = k + 1$ changes lower limit to 1 and upper limit to 7

Changes term to $\frac{1}{j-1+1} = \frac{1}{j}$ to get $\sum_{j=1}^{7} \frac{1}{j}$

- When term references upper limit:

$\sum_{k=1}^{n+1} \left(\frac{k}{n+k}\right)$ to change $j = k - 1$

new lower limit is 0, new upper limit is $n+1 - 1 = n$

This sum regards n as a constant, so $\frac{k}{n+k} = \frac{j+1}{n+j+1}$

$$\sum_{k=1}^{n+1} \left(\frac{k}{n+k}\right) = \sum_{k=0}^{n} \left(\frac{k+1}{n+k+1}\right)$$

Fall 2023 CSCI 150 24/29

24

Properties of Σ

For sequences of reals $(a_m, a_{m+1}, a_{m,+2}, \dots)$ and $(b_m, b_{m+1}, b_{m+2}, \dots)$, $c \in \boldsymbol{R}$

$\sum_{k=m}^{n} c = c(n-m+1)$ (why?)

Let $c = 2, m = 4, n = 6$. $\sum_{k=4}^{6} 2 = 2(6-4+1)$

$\sum_{k=m}^{n} ca_k = c \cdot \sum_{k=m}^{n} a_k$

Let $c = 2, a_k = k+1\ \forall$ integers k from m to n

$\sum_{k=m}^{n} 2(k+1) = \sum_{k=m}^{n}(2k+2) = \sum_{k=m}^{n} 2k + \sum_{k=m}^{n} 2$

$= 2\sum_{k=m}^{n} k + 2(n-m+1)$ (why?)

$\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n}(a_k + b_k)$

To apply this, the upper and lower limits and the index must be the same.

Let $b_k = k+2$.

$\sum_{k=m}^{n}(k+1) + \sum_{k=m}^{n}(k+2) = \sum_{k=m}^{n}(2k+3)$

Application: loops have dummy variables too

Sequences are typically stored in vectors (one-dimensional arrays)

All these produce the same output

for $i := 1$ to $\boldsymbol{n}$
  print $a[i]$
next i

for $j := 0$ to $\boldsymbol{n-1}$
  print $a[j+1]$
next j

for $k := 2$ to $\boldsymbol{n+1}$
  print $a[k-1]$
next k

Product with Π

$$\prod_{k=m}^{n} a_k = a_m a_{m+1} \dots a_n$$

denotes the product of the terms from the lower limit $k = m$ to the upper limit $k = n$ of a_k

$$\prod_{k=2}^{5} k = 2 \cdot 3 \cdot 4 \cdot 5$$

$$\prod_{j=2}^{3} \frac{j}{j-1} = \frac{2}{2-1} \cdot \frac{3}{3-1}$$

If you really care about what number results, use a computer.
What CSCI cares about is your thought process

Properties of Π

For sequences of reals $(a_m, a_{m+1}, a_{m,+2}, \dots)$ and $(b_m, b_{m+1}, b_{m+2}, \dots)$, $c \in \boldsymbol{R}$

$$\prod_{k=m}^{n} c = c^{n-m+1}$$

Let $c = 2, m = 4, n = 6.$ $\prod_{k=4}^{6} 2 = 2^{6-2+1}$

$$\prod_{k=m}^{n} c \cdot a_k = c^{n-m+1} \prod_{k=m}^{n} a_k$$

Let $c = 2, a_k = k + 1 \ \forall$ integers k.
$\prod_{k=m}^{n} 2(k+1) = 2^{n-m+1} \prod_{k=m}^{n} (k+1)$

$$\left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right) = \prod_{k=m}^{n} a_k \cdot b_k$$

To apply this, the upper and lower limits and the index must be the same.

Let $b_k = k + 2$.
$\left(\prod_{k=m}^{n} (k+1)\right) \cdot \left(\prod_{k=m}^{n} (k+2)\right) = \prod_{k=m}^{n} (k^2 + 3k + 2)$

What you should know

- ★ **Real datasets often have exploitable patterns**
- Why $\sqrt{2}$ is irrational
- Why there are infinitely many primes
- How to represent and manipulate finite and infinite sequences

Any questions?

Next up: *Induction*

Time to finish up that Opening sheet!

Problem set 9,10 is due on Monday, October 9 at 11PM

Fall 2023 CSCI 150 29/29

29

Attention

- Every substantive textbook has mistakes, known as *errata*. They are found for years by multiple people and are eventually corrected by the author in a subsequent printing or an online list.
- In case there are others we haven't caught (I've avoided some of them), you should download this errata list and check it regularly: https://condor.depaul.edu/sepp/Errata4e.pdf
- Huasheng Ni caught such an error in Problem Set 7,8 Exercise 4.24. Thank you, Huasheng!
- The corrected question should read:
  "if $m \bmod 5 = 2$ and $n \bmod 5 = 1$ then $mn \bmod 5 = 2$".

Fall 2023 CSCI 150

30