January 11th, 2021
Lior Silberman

1 lior@math.ubc.ca; http://www.math.ubc.ca/~lior/
http://www.math.ubc.ca/~lior/teaching/2021/223_W01/

This PDF is licensed under the terms of the Creative Commons Attribution-Share Alike 3.0 Unported license.
Numbers ???

Number systems
- Natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$
- Integers (whole numbers) $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$
- Rational numbers $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b > 0\}$.
- ... 

Types of numbers
- Prime numbers
- Irrational numbers
- Algebraic numbers
Classical "Theory of Numbers"

- There are infinitely many primes
- The number $\sqrt{2}$ is irrational
- The numbers $e, \pi$ are transcendental (can’t have $\sum_{k=0}^{n} a_k e^k = 0$ with $a_k \in \mathbb{Z}$ unless all $a_i = 0$).
- Every positive integer is the sum of four squares ($30 = 1^2 + 2^2 + 3^2 + 4^2$)
- Every odd integer $\geq 7$ is the sum of three primes ($69 = 17 + 23 + 29$)
- The only integer solutions to $x^p + y^p = z^p$ with $p \geq 3$ have $xyz = 0$. 
Applied number theory

- The largest employer of mathematicians in North America is ...

- Can use number theory to:
  - Establish identity (is https://www.yourbank.ca really my bank?)
  - Maintain privacy (can someone read my communications with the bank?)
  - Distribute secrets
Today’s Goals

1. About the course
2. Learning methods
3. About me
4. Induction
Learning goals

D Basic computational skills (modular arithmetic, cryptography)
   Basic notions and basic implications.
C Definitions, Theorems, direct applications
B Abstract reasoning
A Mastery of course material
A+ General Problem-solving
Course plan

- The Integers
- Congruences and modular arithmetic
- Arithmetic functions
- Applications to cryptography
- The multiplicative group
Components of the course

- Classes (MWF 9:00-9:50)
- Office hours (MWF 11:15-12:00 and Tuesday nights)
- Practice homework (not for submission)
- ComPair homework \[5 \times 4\% = 20\%\]
- Mid-term tests \[4 \times 15\% = 60\%\]
- Final exam [20%]
- Piazza
How to work

- Read before class
- Mindful learning in and out of class
- Solve problem rather than review notes
- Come to office hours & use discussion board
- **ASK QUESTIONS**

Abducted by an alien circus company, Professor Doyle is forced to write calculus equations in the centre ring.

(Gary Larson, “The Far Side”, 15/9/1992)
About me

- Dr. Lior Silberman (Li’or Zilberman)
- Email: lior@math.ubc.ca, Office: MATH 229B.
- Work: Number Theory, PDE, Topology, Random Structures, ...