Discrete Mathematics for High School: A Problem-Based Approach

Mike Pugliese
Arvada West High School

About the Course

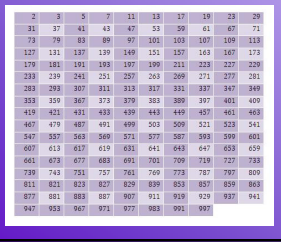
- One semester
- Topics covered
  - **Combinatorics and Discrete Probability**
  - **Number Theory and Cryptography**
  - **Graph Theory**

About the Students

- Post Algebra II
  - required C or better
- C-average Algebra II grades
  - mean grade point=2.4, sd=0.9
- 50% have taken pre-Calculus
  - mean grade point=2.05, sd=1.0
- Average Math ACT scores
  - mean score=20.64, sd=3.58

Today's Objectives

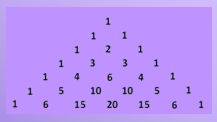
- Work problems used in the class
- Model class practices
- Have fun doing mathematics

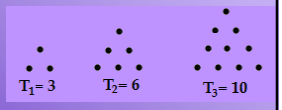


2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997		

Preliminaries

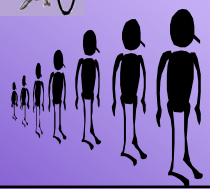
- The Name Game
  - Gaussian sums
- Pascal's Triangle
  - Patterns
  - Binomial expansions
- Figurate Numbers
- Finite differences





Combinatorics and Discrete Probability

- Permutations
- Combinations
- General counting
- Pigeon hole problems
- Advanced counting
- Discrete Probability

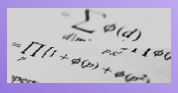


Number Theory and Cryptography

- Properties of prime numbers
- Euler totient function
- Euclidean algorithm
- Cryptography
- Linear congruences
- Modular arithmetic
- Public key encryption

2, 3, 5, 7, 11, 13, 17…

gcd(p_1, p_2) = 1

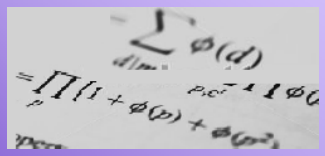


Graph Theory

- Graph Terms and Definitions
- Euler Paths and Circuits
- Hamilton Paths
- Spanning Trees
- Scheduling Problems
- Planar Graphs

Problems in Number Theory and Cryptography

2, 3, 5, 7, 11, 13, 17…



$\gcd(p_1, p_2) = 1$

Linear Congruences
Fred's Baseball Cards

When Fred places his collection of baseball cards in piles of two he has one card left over at the end.

When he lays them out in piles of three he again has one left over.

He tries one more time, using piles of four; once again he has one card left over.

Exasperated, Fred gathers up his cards, lays them out in piles of seven, and this time he has no cards left over.

How many baseball cards does Fred own?

Linear Congruences
Broken Eggs

An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought.

She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

Linear Congruence

- The formal definition of congruence is…

If *a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides a - b.*

This is written $a \equiv b \pmod{m}$.

Modulo Arithmetic

• What do addition and multiplication tables look like for arithmetic mod 3?

•What about for arithmetic mod 5?

Bag Exchange Investigation

Objective: For Alice and Bob to pass two bags through the class and end up with exactly the same content in their bags.

Rules:
1) Bob and Alice secretly place content into their bags
2) No one may look inside the bags
3) Any group may obtain a copy of Alice's or Bob's bag
4) Any group may add content to their copies
5) Alice's and Bob's bag must be passed across the class

Bag Exchange Investigation

Objective: For Alice and Bob to pass two bags through the class and end up with exactly the same content in their bags.

How can Alice and Bob always be sure to end up with the same content in the exchanged bags?

Diffie-Hellman Exchange

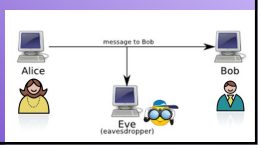
Objective: For two parties to securely obtain a private key for encryption without physically exchanging anything.

Example: Alice and Bob agree to use to values, say

g = 5 and p = 11

Anyone, including Eve can know these values.

The one requirement is that g < p.



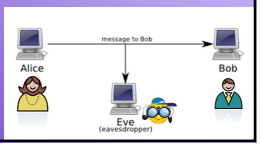
Diffie-Hellman Exchange

Objective: For two parties to securely obtain a private key for encryption without physically exchanging anything.

Example: Alice and Bob now select their own secret key values.

Alice selects 2 as her secret key (k_a), so $k_a = 2$

Bob selects 3 as his secret key (k_b), so $k_b = 3$



Diffie-Hellman Exchange

Objective: For two parties to securely obtain a private key for encryption without physically exchanging anything.

Example: Alice and Bob each calculate an intermediate number using the values of g and p, which are publicly known.

Both use the formula $i \equiv g^k \bmod p$.

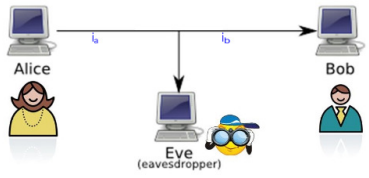
Alice computes $i_a \equiv 5^2 \bmod 11$, so $i_a = \_?$

Bob computes $i_b \equiv 5^3 \bmod 11$, so $i_b = \_?$

Diffie-Hellman Exchange

Objective: For two parties to securely obtain a private key for encryption without physically exchanging anything.

Example: Alice and Bob exchange their intermediate values. Again, Eve can see the intermediate values.



Diffie-Hellman Exchange

Objective: For two parties to securely obtain a private key for encryption without physically exchanging anything.

Example: Alice and Bob compute final values using the formula $K \equiv i^k \bmod p$.

Alice computes $K \equiv i_b^{ka} \bmod p$, so
$K \equiv 4^2 \bmod 11$, $K = \_?$

Bob computes $K \equiv i_a^{kb} \bmod p$, so
$K \equiv 3^3 \bmod 11$, $K = \_?$

Diffie-Hellman Exchange

Objective: For two parties to securely obtain a private key for encryption without physically exchanging anything.

Why do Alice and Bob end up with the same private key value?

Think of the various properties of congruences that we learned.

Diffie-Hellman Exchange

Objective: For two parties to securely obtain a private key for encryption without physically exchanging anything.

What is the relationship of

$g^{ka \times kb} \bmod p$

to

$i_a^{kb} \bmod p$ and $i_b^{ka} \bmod p$

Diffie-Hellman Exchange

Here are the steps:

1) Agree to use to values g and p where $g < p$
2) Select your own secret key value k
3) Computer your intermediate value $i \equiv g^k \bmod p$
4) Pass openly your intermediate value to your partner
5) Compute your private key value using $K \equiv i^k \bmod p$

Work in groups of three. One person is Alice, one is Bob and one is Eve.

Eve's objective is to figure out the private key value.

Diffie-Hellman Exchange

What can be done to make the exchange more secure?

Diffie-Hellman Exchange

Using large values for p make it difficult crack the code, even with a computer.

Try the exchange process again, but use a large value for p.

Since we are using calculators and not computers, we don't need to go to 100s of digits.

Did your exchange remain secure?

Student Comments

- Class was hard to understand; it really takes a deeper thinking
- What we learned was pretty tough
- Good class, enjoyed learning about all these completely new things
- Totally different way of thinking about math
- Overall I had a great time in here even though it was very hard to understand
- Some days fun but some topics made me want to cry
- I wish my last 3 years were taught that way
- Best math class I have ever taken

Resources

- Blog details lessons and mathematics
  - **Pdogmath.blogspot.com**
- Course website contains lesson slides
  - **tinyurl.com/pdogmath**
- NCTM publications
  - Mathematics Teacher
  - Navigating Through Discrete Mathematics in Grades 9-12

Thank you for spending your time exploring discrete math with me!

Mike Pugliese
Arvada West High School
Arvada, CO
mpuglies@jeffcoschools.us
Or
pdogmath@gmail.com