

Mathematical Puzzles, Games and Other Diversions

Day 17

Derrick Chung

April 7 2020

Notes

Problem Solving

From *How To Solve It* (1945) by George Polya



G. PÓLYA, 1887–1985

Four Principles

1. Understand the Problem
2. Devise a Plan
3. Carry Out The Plan
4. Review (and Generalize)

Notes

Problem Solving (cont.)

1. Understand the Problem

This seems so obvious, but it's not. And if you don't really understand the problem, there's no way you can answer it properly.

Some Good Questions

- ▶ Do you understand all the words and notation?
- ▶ What's the goal? What are you being asked?
- ▶ Can you restate the problem in your own words?
- ▶ Would drawing a picture or diagram help your understanding?
- ▶ Is there enough information to enable you to find a solution?

Don't overlook this step. You do so at your own peril.

Notes

Problem Solving (cont.)

2. Devise a Plan

Now figure out how you're going to attack the problem. Choosing an appropriate strategy gets easier with thoughtful practice.

Some Examples

- ▶ Guess and Check
- ▶ Make an ordered list
- ▶ Use symmetry
- ▶ Solve a simpler version
- ▶ Look for a pattern
- ▶ Draw a picture/diagram
- ▶ Solve an Equation
- ▶ Work backward
- ▶ Use a formula
- ▶ Be Creative

This is hard work, so be patient with yourself.
Ideas often need to simmer.

Notes

Problem Solving (cont.)

3. Carry Out the Plan

Following through on your plan is the easy part, if you've got the skills. It will just take some care and patience.

And if your plan isn't working out, go back and make a new plan. It's normal that plans don't work out. Just keep at it.

4. Review (and Generalize)

- ▶ Check your work to make sure you've solved the problem.
- ▶ Reflect on what you've done, what worked and what didn't.
- ▶ Think about other problems where your ideas could be useful.

This step is vital for you to get better at solving problems in the future. Don't ignore it.

Notes

Problem Solving (cont.)

Addendum

“If you cannot solve the proposed problem, try to solve first some related problem. Could you imagine a more accessible related problem?”

Final Considerations

- ▶ You should be considering these principles when you’re solving any math problem.
- ▶ Great mathematicians have followed Polya’s guidance to make important discoveries.
- ▶ The general principles apply beyond just math.

Notes

Intro to Modular Arithmetic

Definition

Let m be a positive integer (called the *modulus*), and let a and b be any integers. Then we say that a is *equivalent* to b modulo m , denoted

$$a \equiv b \pmod{m}$$

if and only if their difference $a - b$ is a multiple of m .

In other words, a and b are equivalent modulo m exactly when a and b have the same remainder after division by the modulus m .

For any modulus m , every integer is equivalent modulo m to exactly one of $0, 1, 2, \dots, m - 1$. We call this number the *residue* of a modulo m .

Notes

Intro to Modular Arithmetic (cont.)

Examples

- ▶ $17 \equiv 5 \pmod{12}$ $20 \equiv 8 \pmod{12}$
- ▶ $23 \equiv 1985 \equiv -11 \equiv 1 \pmod{2}$
- ▶ $65 \equiv 39 \equiv 13 \pmod{26}$.

For convenience, we usually use $a \pmod{n}$ to denote the residue of a modulo n , (i.e. the remainder).

Some Basic Properties

- ▶ $a \pmod{n} + b \pmod{n} \equiv (a + b) \pmod{n}$
- ▶ $a \pmod{n} \cdot b \pmod{n} \equiv (a \cdot b) \pmod{n}$

Notes

Modular Arithmetic (cont.)

For our purposes, we'll be working modulo 26. The substitution table below shows how to transform any message into a sequence of residues modulo 26 (ignoring spacing and punctuation).

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

For instance, the word *BAR* would be converted to **2 1 18**.
And *PIZZA* would become **16 9 0 0 1**.

Instead of using the table, the mnemonic EJOTY is really useful.

$$E = 5 \quad J = 10 \quad O = 15 \quad T = 20 \quad Y = 25$$

Notes

Basic Cryptography

The Caesar Shift Cipher

Messages are encrypted one letter x at a time by shifting each number by n positions to the right.

Described mathematically: $E_n(x) = (x + n) \pmod{26}$. And for decryption, $D_n(x) = (x - n) \pmod{26}$.

Example

Suppose we want to encrypt *PIZZA* by a right-shift of 12.

- ▶ We first write it as numbers: 16 9 0 0 1.
- ▶ We apply $E_{12}(x) = x + 12 \pmod{26}$ to each of the numbers.
- ▶ This gives us 2 21 12 12 13
- ▶ Converting back to letter gives us the encrypted word *BULLM*

Notes

Basic Cryptography (cont.)

Example (cont.)

To decrypt *BULLM* we would simply shift left by 12, using $D_{12}(x) = x - 12 \pmod{26}$ to each of the corresponding numbers to the letters in the word, and that will give us back our original word pizza.

Example

Let's try to decrypt the word *VJCQ* that was encoded with a shift to the right by 9 i.e. applying $E_9(x) = x + 9 \pmod{26}$

- ▶ Convert the letters to numbers: 22 10 3 17
- ▶ Figure out the decryption function: $D_9(x) = (x - 9) \pmod{26}$
- ▶ Apply the decryption function to each number: 13 1 20 8
- ▶ Convert the numbers back to letters: *MATH*

Notes

Basic Cryptography (cont.)

Issues to Consider

- ▶ The encryption is very weak. Only 26 (really 25) ways to encode a message. Easy to crack by brute force.
- ▶ We can use a plain substitution cipher, giving us 26! possibilities.
 - ▶ Takes much longer to crack by brute force.
 - ▶ You have to store much more secret key information: 26 numbers instead of just one.
 - ▶ It also takes longer to encode, since you have to constantly look up the substitution table.
- ▶ How do we improve on the Caesar cipher without increasing our workload too much? We use the *Affine cipher*

Notes
