ICTS-RRI Math Circle, Saturday 11th March 2023

Sam

March 8, 2023

We are spending a few sessions on cryptography and modular arithmetic. As you already realise, modular arithmetic is not just an idle curiosity but has real applications in cryptography. In the next session, we will go deeper into both these topics.

At the end of this note, you will find a write-up on how we learn to solve problems. This is a condensation of some ideas due to the mathematician George Polya. Read through this as a preparation for the session on Saturday. Also please bring along some loose sheets of paper, pencils or pens and a ruler.

First Activity: Here are a few puzzles related to modular arithmetic. 1. In cryptography, we will need to take large powers of numbers (modulo n). Devise a method to calculate these powers efficiently. Do this both analytically as well as using a calculator. Computing 2^{32}modulo11 would be a good start.

2. Fermat's Little Theorem: Last time we played with numbers and arrived at the statement of Fermat's Little Theorem: For p prime

$$a^p = a \text{ modulo } p \quad (1)$$

Prove this statement. (Hint: use induction on a). Numbers n which do not satisfy $a^n = a$ modulo n are definitely composite and this can help in distinguishing between primes and composites. The converse is not true! There are composite numbers n, which satisfy this equation for all a. These are called Carmichael numbers. 1729 is one such.

Tea break: 11:15

Second Activity Codes: We saw last time that substitution ciphers were susceptible to frequency analysis. We then looked at running key ciphers. These too are vulnerable and we will discuss why. Finally, we will look at Vernam Ciphers (the one-time pad) and discuss its weaknesses. All this is preparation for the next session where we will discuss Public Key Cryptography (RSA) and Quantum Key distribution.

How to Solve it? by George Polya

This writeup explains in simple language Polya's method for solving problems. All of us are faced with problems in everyday life and we use a number of tricks to solve them. For instance, you come home from school and find the front door locked and nobody home. What do you do? Think hard. Is there a friendly neighbour? Could there be a window open? Would they have left the key in a hiding place? Can I reach them on the phone? As we get older we get better and better at solving life's problems. We learn from past experience and develop a bag of tricks.

The same is true for problems in mathematics or physics. Many of us use these tricks without being aware that we are using them. For those of you who are learning to solve problems, it is useful to make these rules explicit. This is what George Polya, a Hungarian Mathematician did in a book called "How to solve it?". What follows is a simplified and condensed version of Polya's ideas.

The process is divided into four steps: Understand, Plan, Solve and Review. When you start, you will slowly and consciously go through these steps. As you get more experienced, you will use this method without even thinking about it.

1. *Understand the Problem:* It goes without saying that in order to solve a problem we have to understand it. Here are questions that you ask yourself in order to do this:

    - What form will the answer take? Is it a number, a length? Or is it a logical argument? A proof? An algorithm? A strategy?
    - What is the data that is given to me? Scan the statement of the problem to isolate the data.
    - What are the conditions of the problem? For instance, the answer may have to be a whole number. Or, in a logical proof, the statement may apply only to polygons.

2. *Planning an attack on the Problem:* Ask yourself these questions:

    - Have I seen a related problem before? A problem with a similar unknown?
    - How is the data related to the unknown? Is there too little data? Too much data?
    - Can I simplify the problem by considering a special case? an extreme case?
    - Can I simplify the problem by making it more general?
    - Can I give up a condition? Eg. give up the condition that the answer has to be a whole number and solve it with real numbers.
    - In some problems (a maze for example), it is advantageous to work backwards: start from the end, assuming we have reached our goal. Would this work in our problem?
    - Are there obvious symmetries in the problem?

3. *Solve* In this step, we implement the plan devised in the last section. This may involve calculation or developing the logical steps of a proof. It may be that the first attempt does not succeed. If so we go back to the planning stage and refine it.

4. *Review* This step is important for you to develop problem-solving skills for the future. Don't regard a solved problem as dead. You can learn a lot from problems you have already solved and use this knowledge in the future. Ask yourself

    - is there a way to check the solution?
    - Can the solution be generalised?
    - Can I use the solution to devise new problems?

    The next time you are faced with a problem, (even a simple one) try to go through these steps and learn from them. With practice, you will find your skills improving. Good luck!