A glimpse of sample topics

- *Elementary number theory.* A positive integer $n > 1$ is *prime* if it is exactly divisible only by 1 and by itself; for example $2, 3, 5, 7, 11, 13, 17, ...$ are primes, while 6 is not. These are the basic building blocks in number theory. Can you prove that there are infinitely many prime numbers? This we will discuss at the very beginning of our course. Can you prove that there are infinitely many primes, whose last digit is 1, such as $11, 31, 41, 61, 71, 101$? This we will discuss much later in the course, as it requires developing more advanced techniques. But, along the way of establishing these techniques, we will have learned a lot about number theory, and when we arrive at the proof, we will have the satisfaction of the accomplishment of a long–term project. Can you prove that there are infinitely many primes, whose last digit is 3? This is too deep and difficult, hence beyond our scope; however, it illustrates how easy it is to ask a question in number theory that can turn out to be highly nontrivial.

  Prime numbers have practical applications as well: they are used for the secure exchange of communication in cryprography. For example, any time when you enter a password on a webpage, there are prime numbers behind the curtains that enable you to send the information securely. Here is a lecture on this topic that I had given in the past: `https://www.youtube.com/watch?v=bE_N697l7wk` (you will be able to understand it easily after we build some foundation). Our emphasis will be on the theoretical aspects but such applications will be touched upon as well.

  You have a lot of experience in solving equations in just one variable, such as $x^4 + x^3 - 3x^2 - 5x - 10$, or $x^2 - 5 = 0$. But what if you try to study equations in more than one variables, imposing the condition that the unknowns are *integers*? These are called *Diophantine* equations, and there is no general routine method for solving them. Can you prove that $\sqrt{2}$ is irrational, i.e., that it cannot be written as a fraction $\frac{x}{y}$ with x, y integers – equivalently, that one cannot find integers $x, y \geq 1$ such that $x^2 = 2y^2$? This will be easy. A harder question is: describe all "Pythagorean" triples (x, y, z) of integers such that $x^2 + y^2 = z^2$; for example: $3^2 + 4^2 = 5^2, 5^2 + 12^2 = 13^2$. Even harder is the following question: can you find integers x, y such that $x^2 - 217y^2 = 1$? Surprisingly, to answer this, we will need to build geometric arguments, in the spirit of the following question: Take an infinite grid of unit squares in the plane, and around each point, imagine a small rabbit, represented by a disc of tiny radius r, say $r = 0.000001$. A hunter is located at one of the grid points and shoots randomly. Will the hunter necessarily hit some rabbit?

- *Complex numbers.* Is there a number z such that $z^2 = -1$? Well, one can *build* a system of numbers, in which the answer to this question is "yes." These numbers will correspond no longer to points on a line, but to points in the plane. They are extremely useful and have a variety of applications, ranging from plane geometry to number theory and beyond. For example, draw 4 circles $C_1, ..., C_4$ in the plane, so that C_1 and C_2 intersect in 2 points P_1, Q_1; C_2 and C_3 intersect in 2 points P_2, Q_2; C_3 and C_4 intersect in 2 points P_3, Q_3; and, finally, C_4 and C_1 intersect in 2 points P_4, Q_4. If P_1, P_2, P_3, P_4 lie on a line or a circle, then so do Q_1, Q_2, Q_3, Q_4. This is very elegant and easy, when one uses complex numbers.

- *Graph theory and combinatorics.* If there are 6 people in a company, there are either 3, among which any two know each other, or 3, among which no two know each other. Can you prove this? A triple of one of the above two types is called a "monochromatic" triple. Can you prove that in fact, there are at least 2 such monochromatic triples, in any company of 6? These are often the first two problems in *graph theory* that one encounters. But later, we will move to more complicated ones: if there is a company of n people, with no "p-clique" (i.e., no p of them, among which anyone knows the other $p-1$), what is the largest number of acquaintance pairs in this company?

  Combinatorial geometry problems and techniques will also be discussed. For example, suppose you have a museum with the shape of a polygon with 24 sides. You want to place guards in the museum at certain points; the guards cannot move but can turn by 360° at any direction. Can you prove that 8 guards will suffice, no matter how complicated the shape of the museum is? We will see how the method used to answer this question can be applied in many other problems concerning regions in the plane.

- *Generating functions.* Consider the sequence defined as follows: $a_0 = 1, a_{n+1} = 2a_n + n$ for $n \geq 0$. Here are the first few terms: $1, 2, 5, 12, 27, 58, ...$ Can you find a (simple) formula for a_n? The method of generating functions is a technique for handling questions of this type. The advantage of using this method over examining the pattern and coming up with the answer $a_n = 2^{n+1} - n - 1$ is that the solution does not come just "out of nowhere" but is produced by a uniform technique.

  As another application, one can easily solve the following counting problem: say n family couples go to a party. In how many ways can one arrange that they dance in pairs, so that noone dances with their original partner? Or, say that a certain bank issues only coins of 3 cents and 5 cents. In how many ways can one change an amount of N cents into coins?

- *Inversion in plane geometry.* Draw two circles C_1 and C_2, tangent to each other at a point R_0, with C_2 inside C_1. In the region enclosed by C_1 and C_2, draw a circle D_0 tangent to both C_1 and C_2. Next, draw a circle D_1 tangent to C_1, C_2, and D_0, and let R_1 be the point of tangency of D_1 and D_0. Next, draw a circle D_2, tangent to all C_1, C_2, and D_1, with R_2 the point of tangency of D_2 and D_1. Continue in this way to construct circles $D_1, D_2, ...$ and points of tangency $R_1, R_2, ...$ Can you prove that all points $R_1, R_2, ...$, and R_0 lie on a single circle? This becomes very easy, if one applies "inversion": this is a tool that allows one to transform a complicated geometric configuration into another, often easier, configuration, in which some of the circles get replaced by lines. The advantage is that lines are easier to handle than circles. There are numerous applications of inversion to complicated settings where many circles are involved. The proofs are often quite short and elegant.