Lecture 10: Pigeonhole principle, Basic number theory

Nitin Saxena ⋆

IIT Kanpur

The pigeonhole principle can be extended slightly, with the same proof (show it).

Theorem 1. *If there are $rn+1$ pigeons and n pigeonholes then at least one pigeonhole will have more than $r+1$ pigeons.*

Example 1. Given 6 vertices of a hexagon, join all pairs of vertices by either red or blue edge. Show that there is at least one monochromatic triangle (all edges of the same color).

Choose a vertex v. There are 5 edges going from it. Since there are 2 colors, at least three edges are of the same color by the new pigeonhole principle. Suppose these 3 edges are of red color and go to vertices v_1, v_2, v_3.

There are 3 edges between v_1, v_2, v_3. If all of them are blue then we have a monochromatic blue triangle (v_1, v_2, v_3). Otherwise, say, v_1, v_2 is red and then v, v_1, v_2 triangle is all red. Hence proved.

Exercise 1. Color the edges of a pentagon such that there is no monochromatic triangle.

Exercise 2. Read about Ramsey numbers.

$R(m,n)$ is the minimum number of vertices required in a graph G so that: Either G has an m-clique or an n-independent set. We showed above that $R(3,3) = 6$.

Exercise 3. Give a combinatorial argument for the recurrence,

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

1 Basic number theory

In the next few classes we will talk about the basics of *number theory*. Number theory studies the properties of natural numbers and is considered one of the most beautiful branches of mathematics. In this lecture note, numbers means natural numbers or integers depending upon the context.

The first goal for us would be to prove that every number has a unique prime factorization (*fundamental theorem of arithmetic*), using the basic division algorithm.

1.1 Division algorithm

Division algorithm says that given two numbers a and b, we can divide a by b obtaining quotient q and remainder $0 \le r < b$:

$$a = qb + r\,.$$

Eg. $101 = 7 \cdot 14 + 3$.

Exercise 4. Show that the quotient and the remainder are unique if we assume that the remainder is less than b.

Suppose not. Then, $a = qb + r = q'b + r'$, implying that $(q - q')b + (r - r') = 0$. The latter gives $b|(r - r')$, but we had assumed that $0 \le r, r' < b$. This contradiction implies uniqueness.

⋆ Edited from Rajat Mittal's notes.

A number b *divides* a if the remainder is zero. We denote it by $b \mid a$. Similarly, $b \nmid a$ denotes that b does not divide a. If b divides a then a is a *multiple* of b. Eg. $7 \nmid 101$, $7|105$.

Now we can define the *greatest common divisor (GCD)*. The GCD of two numbers a and b is defined as the biggest number which divides both a as well as b. It is also denoted by $\gcd(a, b)$.

One of the important cases is when $\gcd(a, b) = 1$, i.e. there is no common factor between a and b. We say that a and b are *coprime* to each other.

1.2 Euclid's GCD algorithm (c.300 BC)

Euclid's GCD algorithm is one of the earliest, most elementary and most important algorithm in the world of mathematics. It gives a recursive way to calculate the GCD.

Suppose we are given two numbers a, b s.t. $a \geq b \geq 0$. The algorithm $\gcd(a, b)$ is given below.

if $b = 0$ **then**
 | Output a
end
if $b = 1$ **then**
 | Output 1
end
Compute $a = qb + r$ by the division algorithm. Output $\gcd(b, r)$.

Algorithm 1: GCD algorithm

The correctness of the procedure relies on the fundamental fact that if $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Exercise 5. Can you prove this?

$$\gcd(a, b) = \gcd(a, a + qb) = \gcd(r, b) \cdot$$

To take an example, let us compute the GCD of 64 and 26.

$$\begin{aligned} \gcd(64, 26) &\to 64 = 2 \times 26 + 12 \\ \gcd(26, 12) &\to 26 = 2 \times 12 + 2 \\ \gcd(12, 2) &\to 12 = 6 \times 2 + 0 \\ \gcd(2, 0) &\to 2. \end{aligned} \tag{1}$$

This shows that $\gcd(64, 26) = 2$. In general, the equations will look like,

$$\begin{aligned} \gcd(a, b) &\to a = q_1 \times b + r_1 \\ \gcd(b, r_1) &\to b = q_2 \times r_1 + r_2 \\ &\vdots \\ \gcd(r_{k-2}, r_{k-1}) &\to r_{k-2} = q_k \times r_{k-1} + r_k \\ \gcd(r_{k-1}, r_k) &\to r_{k-1} = q_{k+1} \times r_k + 0 \\ \gcd(r_k, 0) &\to r_k. \end{aligned} \tag{2}$$

In this case $\gcd(a, b)$ will be r_k. Notice that r_1 can be written as an integer combination of a, b, i.e., $r_1 = c_1 a + c_2 b$ for some integers c_1, c_2 using the first equation. Similarly r_2 can be written as an integer combination of b, r_1 and hence a, b.

Keeping track of these coefficients (i.e. by induction), ultimately we can write the $\gcd(a, b) = r_k$ as the integer combination of a, b.

Exercise 6. What can you say about the number of steps in Euclid's algorithm?

Hint: It's related to the Fibonacci sequence!

Exercise 7. Write the pseudocode of the other version of Euclid's algorithm in which we halve the smaller number each time, i.e. we use $a = qb + r$ where $|r| \leq b/2$. How many steps will it take?

References

1. N. L. Biggs. Discrete Mathematics. *Oxford University Press*, 2003.
2. P. J. Cameron. Combinatorics: Topics, Techniques and Algorithms. *Cambridge University Press*, 1994.
3. K. H. Rosen. Discrete Mathematics and Its Applications. *McGraw-Hill*, 1999.