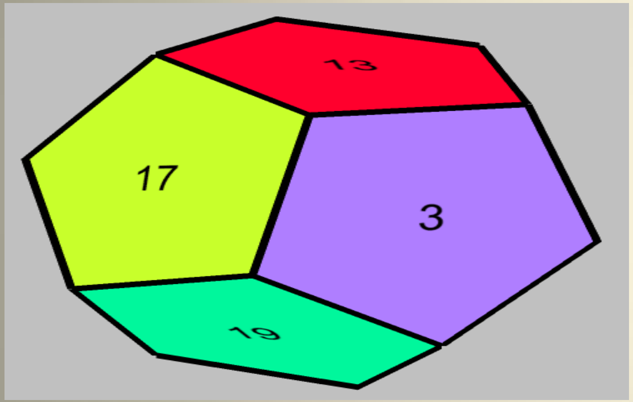
Theory of Prime Numbers: Basics



DR. SHEO KUMAR SINGH
Assistant Professor,
Department of Mathematics
School of Physical Sciences,
Mahatma Gandhi Central University, Motihari, Bihar-845401

Email: sheokumarsingh@mgcub.ac.in

All the numbers discussed in the presentation are natural numbers

- Numbers are essential and more commonly used in our day-to-day life.
- Question is: What is a prime number?
- A number greater than 1 is prime if it cannot be written as a product of two smaller numbers.
  - For example 2, 3, 5, 7, 11, 13, 17, … etc.

Why prime numbers are so important?

- **Fundamental theorem of arithmetic (~300 BCE):**

  Every natural number greater than 1 can be expressed uniquely as the product of primes (up to rearrangement).

  Above result shows that prime numbers are the atomic elements for all natural numbers,

  For example,

  - $6=2\times3$, $10=2\times5$, $15=3\times5$, $40=2\times2\times2\times5$, $100=2\times2\times5\times5$, …

- These are very useful in making (high security) passwords, and the simple reason behind this is the following fact

  - $29\times31=899$, but what about 899= -- × -- ,

- I mean to say that, it is easy to multiply two numbers but very difficult to factorize a number

- **Euclid's theorem (~300 BCE):** There are infinitely many prime numbers.
- Proof (outline):

1. Suppose for contradiction that there are only finitely many primes $p_1, p_2, \ldots, p_n$. (For instance, suppose 2, 3, and 5 were the only primes.)
2. Now multiply all the primes together and add 1, to create a new number $P = p_1\, p_2 \ldots p_n + 1$. (For instance, P could be 2 x 3 x 5 + 1 = 31.)
3. P is then an integer which is larger than 1, but is not divisible by any prime number.
4. But this contradicts the fundamental theorem of arithmetic. Hence there must be infinitely many primes. □

Some famous conjectures

- (Twin-Prime): There are infinitely many pair of primes p & p+2 which differs by exactly 2.
  - For example, (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), (149, 151), (179, 181), (191, 193), (197, 199), … etc.
- (Gold-Bach): Every even number, greater than 2, can be expressed as the sum of two prime numbers.
  - For example, 4=2+2, 6=3+3, 8=3+5, 10=3+7=5+5, 12=5+7, … etc.

- Euclid’s theorem tells us in principle that there are arbitrarily large primes out there, but does not give a recipe to find them.

Formula/technique to know that a given number is prime

– A number $\mathbb{N}$ is prime if it cannot be divisible by any prime $\leq\sqrt{\mathbb{N}}$

- The largest known prime (as of January 2020) is $2^{82,589,933} - 1$, which is 24,862,048 digits long and was found by Patrick Laroche of the GIMPS in 2018.

Unfortunately, still there is no formula or technique to find

- what is the n^{th} prime number p_n ?
- If P is a prime number, then what is the next prime ?

- On the other hand, the primes also have some local structure. For instance,
  - They are all odd (with one exception);
  - They are all adjacent to a multiple of six (with two exceptions);
  - Their last digit is always 1, 3, 7, or 9 (with two exceptions).

- Prime number theorem (Hadamard, de Vallée Poussin, 1896):
  - The n^{th} prime is approximately equal to $n \ln n$.
- The Riemann hypothesis conjectures an even more precise formula for the n^{th} prime.

It remains unsolved; the Clay Mathematics Institute has a US $1,000,000 prize for a correct proof of the above hypothesis.

References:

- Thomas Koshy, Elementary Number Theory with Applications, 2nd ed., Academic Press.
- Niven, Zuckerman and Montgomery, An Introduction to the Theory of Numbers, 5th ed., John Wiley & Sons.
- Terence Tao, Structure and Randomness in the Prime Numbers, Science Colloquium (January 2007).

THANK YOU