APS
Fermat's Little Theorem

Course Code: 17ECSE309

- Akshay Gudiyawar

EC A Division

USN: 01FE15BEC021

Fermat’s Little Theorem

- Intuition

→ It’s a fundamental theorem in elementary number theory, which helps to compute powers of integers modulo prime numbers.

→ It finds great application in generation of pseudo-prime numbers’ and in encryption for generating large prime factors

Fermat's Little Theorem

- Statement : It states that if p is a prime number, then for any integer a, the number a*p − a is an integer multiple of p. In the notation of modular arithmetic, this is expressed as

- Equation: $a^p = a \ (mod \ p \ )$

- Example : If a = 2 and p = 7, then 26 = 64, and 64 − 1 = 63 = 7 × 9 is thus a multiple of 7.

Applications

- The theorem finds many uses in

1. Cryptography - in particular, underlies the computations used in the RSA public key encryption method.
2. Pseudo – primes
3. Number – theory
4. Primality testing – using corollary, we can test whether the given no is prime or composite.

References:

- https://brilliant.org/wiki/fermats-little-theorem/
- https://en.wikipedia.org/wiki/Fermat%27s_little_theorem
- https://www.quora.com/What-are-the-real-life-applications-of-Fermats-little-theorem
- http://mathworld.wolfram.com/FermatsLittleTheorem.html
- http://www.quanta-magazine.com/single-post/2017/08/31/Application-of-Fermats-Little-Theorem

Thank you