Elementary Number Theory: Fermat's Theorem

Arjun Vardhan

†

Created: 16th May 2022
Last updated: 4th July 2022

1 Fermat's Little Theorem and Pseudoprimes

- **Fermat's little theorem: Let p be prime and suppose that p does not divide a. Then $a^{p-1} \equiv 1 \mod p$.** *Proof:*
- **Corollary: If p is prime, then $a^p \equiv a \mod p$ for any integer a.** *Proof:*
- A composite integer n is called a pseudoprime whenever $n \mid 2^n - 2$.
-

2 Wilson's Theorem

- **Wilson's Theorem: If p is prime, then $(p-1)! \equiv -1 \mod p$.** *Proof:*