# Fermat's little theorem

UNIVERSITY OF TORONTO

February 23rd, 2021

# Binomial coefficients

Given $0 \leq k \leq n$ two natural numbers, we denote by $\binom{n}{k}$ (read as "$n$ choose $k$") the number of ways to choose an (unordered) subset of $k$ elements from a fixed set of $n$ elements.

Remember that it satisfies *(proved in class, see the video)*:

- $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
- For $0 \leq k < n$, we have $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$ *(Pascal's triangle)*
- $\forall x, y \in \mathbb{R}, \forall n \in \mathbb{N}, (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ *(Binomial theorem)*

## Lemma

Let $p$ be a prime number. Then $\forall k \in \{1, \ldots, p-1\}$, $\binom{p}{k} \equiv 0 \pmod{p}$.

*Proof.*
Let $k \in \{1, \ldots, p-1\}$. Then $k\binom{p}{k} = p\binom{p-1}{k-1}$. Hence, $p | k\binom{p}{k}$.

Since $\gcd(p, k) = 1$, by Gauss' lemma, we get that $p | \binom{p}{k}$. ∎

## Fermat's little theorem, version 1

Let $p$ be a prime number and $a \in \mathbb{Z}$. Then $a^p \equiv a \pmod p$.

*Proof.* We first prove the theorem for $a \in \mathbb{N}$ by induction.
*Base case at $a = 0$:* $0^p = 0 \equiv 0 \pmod p$.
*Induction step:* assume that $a^p \equiv a \pmod p$ for some $a \in \mathbb{N}$. Then

$$\begin{aligned}(a+1)^p &= \sum_{n=0}^{p} \binom{p}{n} a^n && \text{by the binomial formula}\\ &\equiv a^p + 1 \pmod p && \text{since } p \mid \binom{p}{n} \text{ for } 1 \le n \le p-1\\ &\equiv a + 1 \pmod p && \text{by the induction hypothesis}\end{aligned}$$

Which ends the induction step.

We still need to prove the theorem for $a < 0$.
In this case $-a \in \mathbb{N}$, hence, from the first part of the proof, $(-a)^p \equiv -a \pmod p$.
Multiplying both sides by $(-1)^p$ we get that $a^p \equiv (-1)^{p+1} a \pmod p$.
If $p = 2$ then either $a \equiv 0 \pmod 2$ or $a \equiv 1 \pmod 2$, and the statement holds for both cases.
Otherwise, $p$ is odd, and hence $(-1)^{p+1} = 1$. Thus $a^p \equiv a \pmod p$. ∎

# Fermat's little theorem, version 2

## Fermat's little theorem, version 2

Let $p$ be a prime number and $a \in \mathbb{Z}$. If $\gcd(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod p$.

*Proof.*
By the first version of Fermat's little theorem, $a^p \equiv a \pmod p$.
Hence $p | a^p - a = a(a^{p-1} - 1)$.
Since $\gcd(a, p) = 1$, by Gauss' lemma, $p | a^{p-1} - 1$.
Thus $a^{p-1} \equiv 1 \pmod p$. ∎

## Remark

Note that both versions of Fermat's little theorem are equivalent.