Fermat's little theorem

Seminar on computer-assisted mathematics

Janina Planeta, Julia Renner

$$a^p - a \equiv 0 \pmod{p}$$

Fermat's little theorem

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 arithemtic, this is expressed as $a^p \equiv a \pmod p$.

Modulo operation

$a = p \cdot b + r$, then $a \equiv r \pmod p$

Example: $7 = 2 \cdot 3 + 1 \Rightarrow 7 \equiv 1 \mod 2$

Proof:

Preliminary considerations:

> If a is divisible by p: $a \equiv 0 \equiv a^p \pmod p$

> It is sufficient to consider natural numbers a. For negative integers the statement then follows by considering $-a$ ($a \in \mathbb{N}$).

$p = 2$: $(-a)^2 - (-a) = a^2 + a = a^2 + \underbrace{2a}_{\equiv 0 \pmod 2} - a = a^2 - a$

$p \neq 2$: $(-a)^p - (-a) = (-1)\, a^p - (-1)\, a = -(a^p - a)$

By induction with $a \in \mathbb{N}$.

Base clause:

$0^p - 0 \equiv 0 \pmod p$

Induction hypothesis:

$a^p - a \equiv 0 \pmod p$ for any $a \in \mathbb{N}$.

Induction step:

$$(a+1)^p - (a+1) = a^p + \binom{p}{1} a^{p-1} + \dots + \binom{p}{p-1} a + 1 - (a+1)$$

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!} = \frac{p \cdot (p-1) \cdots (p-k+1)}{1 \cdot 2 \cdot \cdots \cdot k}$$

p only appears in the numerator for $1 \leq k \leq p-1$.

Since p is a prime number, there are no divisors of p in the denominator.

$\Rightarrow \binom{p}{k}$ is therefor divisible by p for $1 \leq k \leq p-1$.

$\Rightarrow \binom{p}{k} \equiv 0 \pmod p$

$\Rightarrow (a+1)^p - (a+1) \equiv a^p + 1 - (a+1) \equiv a^p - a \pmod{p}$

$\overset{IH}{\Rightarrow} (a+1)^p - (a+1) \equiv 0 \pmod{p}$

$\blacksquare$

Alternative proof (Combinatorics)

> Consider a necklace with p beads

> Each bead can be colored in a different ways

$\Rightarrow a^p$ ways to pick the colors of the beads

There are a necklaces where all the beads have the same color.

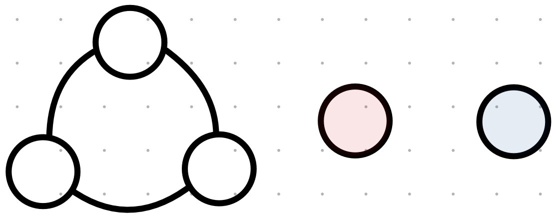
Of the remaining necklaces, for each necklace, there are exactly p-1 necklaces that are rotationally equivalent to this necklace.

$\Rightarrow a^p - a$ must be divisble by p

$\Rightarrow a^p - a \equiv 0 \pmod{p}$

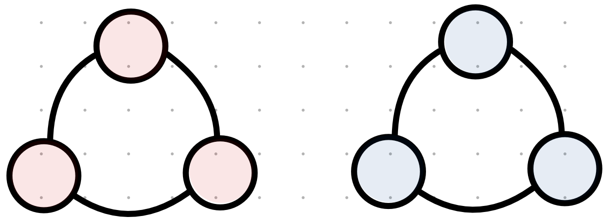
Alternative proof illustrated for $p = 3$ and $a = 2$

Necklace with $p = 3$ beads and $a = 2$ colors:



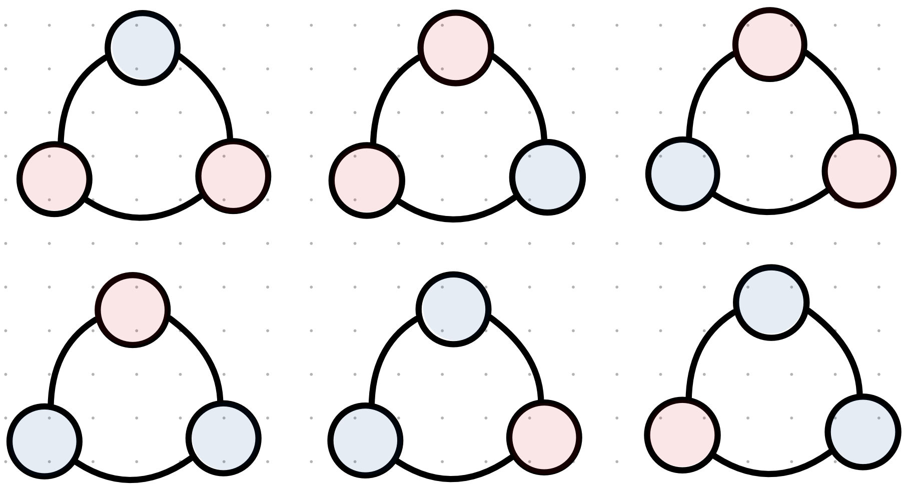
$\Rightarrow$ $a^p = 2^3 = 8$ ways to color them

Necklaces that consists of beads of the same color:



$\Rightarrow$ $a = 2$ necklaces

Necklaces that are rotationally equivalent:



$\Rightarrow$ for each necklace, there are $p-1 = 3-1 = 2$ necklaces that are rotationally equivalent

Examples

(1) $p = 5$ (prime), $a = 2$

$2^5 - 2 = 32 - 2 = 30 \equiv 0 \pmod{5}$

(2) $p = 6$ (not prime), $a = 2$

$2^6 - 2 = 64 - 2 \equiv 2 \neq 0 \pmod{6}$

Applications

> primality testing
> public-key cryptography
> computer security
> internet banking

Funfact

It's a special case of Euler's Theorem: $a^{\varphi(n)} \equiv 1 \bmod n$, where $\varphi(n)$ counts the positive integers up to n, that are relatively prime to n.

Resources

> https://artofproblemsolving.com/wiki/index.php/Fermat%27s_Little_Theorem

> https://testbook.com/maths/fermats-little-theorem#:~:text=Applications%20of%20the%20Theorem&text=Fermat%27s%20Little%20Theorem%20is%20also,%E2%88%921(modn)

> https://de.wikibooks.org/wiki/Beweisarchiv:_Zahlentheorie:_Elementare_Zahlentheorie:_Kleiner_Satz_von_Fermat

> https://en.wikipedia.org/wiki/Fermat%27s_little_theorem

> https://de.wikipedia.org/wiki/Kleiner_fermatscher_Satz