Review of Fermat's Little Theorem
Lecture 10a: 2022-03-21

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Fermat’s little theorem

- Theorem Statement
  - Let p be prime.
  - If $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$.
  - For any a (including 0), can say $a^p \equiv a \pmod{p}$.
- Applications
  - Finding large powers
  - Finding certain roots

Finding large powers

- Algorithm for $a^m \pmod{p}$.
  - Conditions: p is prime and $a \not\equiv 0 \pmod{p}$.
  - Find $m = x(d-1) + r$ by division with remainder.
  - Then $a^m \equiv a^r \pmod{p}$.

Finding certain roots

- Intuition:
  - kth roots are easy for anything written as a^{km}, because $\sqrt[k]{a^{km}} = \left(a^{km}\right)^{\frac{1}{k}} = a^m$.
  - We can rewrite $a^1 \equiv a^{(p-1)l+1}$ for any integer l.

Finding certain roots without lists

- Algorithm for $\sqrt[k]{a} \pmod{p}$
  - Conditions: p is prime, $a \not\equiv 0 \pmod{p}$, and $\gcd(k, p-1) = 1$.
  - Find 1 as a combination of k and $p-1$
  $$1 = km - l(p-1)$$
  - Then $a^1 \equiv a^{1+l(p-1)} \equiv a^{km}$.
  - So $\sqrt[k]{a} \equiv \sqrt[k]{a^{km}} \equiv a^m \pmod{p}$

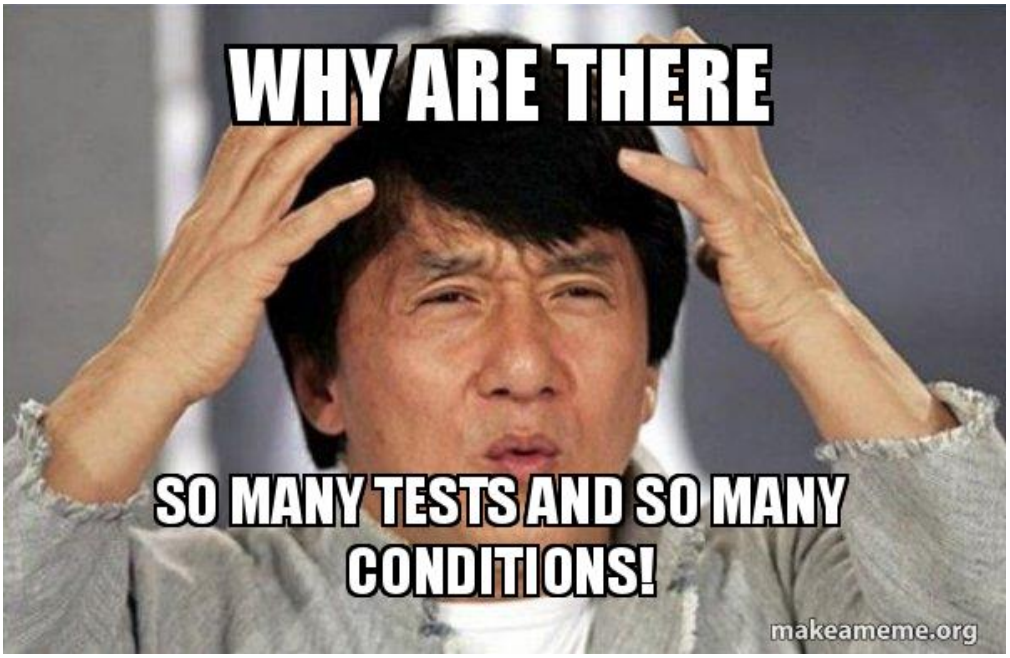
Try out Fermat's Little Theorem

- $3^{1000} \mod 81$
- $2^{666} \mod 61$
- $\sqrt[3]{10} \mod 57$
- $\sqrt[3]{10} \mod 61$
- $\sqrt[3]{10} \mod 11$

A: 2
B: 3
C: 5
D: 10
E: Can't use FLT

Think like a mathematician

- Fermat's Little Theorem and the methods related to it only work under certain conditions, but make things a lot easier when they do.



Think like a mathematician

- Questions:
  - Why do we need the modulus to be prime?
  - Can we sometimes make Fermat's Little Theorem work even when the modulus is not prime?
- Strategies:
  - What are some of the ways we've figured out patterns / things to prove?

Answer in chat

  - Did a lot of experiments, wrote them into tables, and then looked for patterns.
  - Made guesses based on analogies to other similar things (roots are harder because it is reversing something, and we know that subtraction and division are harder).
- Another approach:
  - Carefully studying proof steps.

How we came up with FLT

	a^0	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1	2	4	1	2	4	1
3	1	3	2	6	4	5	1	3	2	6	4	5	1
4	1	4	2	1	4	2	1	4	2	1	4	2	1
5	1	5	4	6	2	3	1	5	4	6	2	3	1
6	1	6	1	6	1	6	1	6	1	6	1	6	1

Proof idea

- Remember from the bean-bag tossing experiment that for prime modulus p, the multiples of any non-zero number x are all the numbers.

Ex. in mod 7, multiples of 2

$2, \quad 4, \quad 6, \quad 8, \quad 10, \quad 12, \quad 14$

$ \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

$ \quad 1 \quad 3 \quad 5 \quad 0$

$12 \equiv 5$

$\frac{12}{6} \equiv \frac{5}{6}$

- Now we write a in $p-1$ different ways:

$$a \equiv \frac{a}{1} \equiv \frac{2a}{2} \equiv \frac{3a}{3} \equiv \cdots \equiv \frac{(p-1)a}{p-1}.$$

Ex. $2 \equiv \frac{2}{1} \equiv \frac{4}{2} \equiv \frac{6}{3} \equiv \cdots \equiv \frac{12}{6}$ mod 7

- Multiplying them all together gives the proof.

$$a^{p-1} \equiv \frac{a}{1}\frac{2a}{2}\frac{3a}{3}\cdots\frac{(p-1)a}{p-1} \equiv 1$$

all the nonzero numbers exactly once

Ex. $2^6 \equiv \frac{2 \cdot 4 \cdot 6 \cdot 1 \cdot 3 \cdot 5}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} \equiv 1$ mod 7

Step 0: list start and end

- Needed: p has to be prime.

- Needed: $a \not\equiv 0 \pmod{p}$

- Claim: $a^{p-1} \equiv 1 \pmod{p}$

Step 1: rewriting a^{p-1}

Step 2: multiples are all numbers

Step 3: multiples go through all non-zero in a cycle before returning to 0

Step 4: putting it all together

Examining the proof

- Step 1 depends on prime p in order to divide.
  - Maybe we can find other circumstances in which we can divide?
- Step 2 uses $a \not\equiv 0 \pmod{p}$ to show that $\gcd(a, p) = 1$, which makes the multiples all possible numbers.
- Step 4 then used the number of non-zero numbers in mod p, which is $p - 1$, as the cycle length $a^{p-1} \equiv 1$.
  - Maybe when we are not working in a prime, we can find some other shorter cycle of multiples that still works?

- Next time: we will show Euler's Theorem, which generalizes Fermat's Little Theorem to non-prime modulus.