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

$$a^{1002} \pmod{11} \equiv a^2 \pmod{11}$$

because $a^{10} \equiv 1$.

  - Finding certain roots

$$\sqrt[3]{a} \pmod{11} \equiv \sqrt[3]{a^{11}} \equiv \sqrt[3]{a^{21}} \equiv a^7 \pmod{11}$$

Finding large powers

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

Ex. $2^{125} \pmod{13} \equiv 2^5 \pmod{13}$

$\equiv 2^4 \cdot 2^1 \pmod{13}$

$\equiv 3 \cdot 2 \pmod{13}$

$\equiv 6 \pmod{13}$

$12 \overline{)125}$ = 10 r 5

12

05

$2^1 \equiv 2$

$2^2 \equiv 4$

$2^4 \equiv 16 \equiv 3$

$\equiv 32 \pmod{13}$

$\equiv 6 \pmod{13}$

Finding certain roots

$11^5 \bmod 17 \equiv 10$

?

$10^1 \equiv 10^1 \cdot 1 \equiv 10^1 \cdot 10^{16} \equiv 10^{17}$

- 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.

Ex. $\sqrt[5]{10} \bmod 17$. Note $10^{16} \equiv 1 \bmod 17$

So $10^1 \equiv 10^{17} \equiv 10^{33} \equiv 10^{49} \equiv 10^{65} \bmod 17$

Thus $\sqrt[5]{10} \equiv \sqrt[5]{10^{65}} \equiv 10^{65/5} \equiv 10^{13} \bmod 17$

$\equiv 10^8 \cdot 10^4 \cdot 10^1$

$\equiv -1 \cdot 4 \cdot 10$

$\equiv -40 \equiv -40 + 17 \cdot 2$

$\equiv -6 \equiv 11 \pmod{17}$

$10^1 \equiv 10$

$10^2 \equiv 100 \equiv 15$

$10^4 \equiv 225 \equiv 4$

$10^8 \equiv 16 \equiv -1$

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 $p-1$
$$1 = km - l(p-1)$$
$1 + l(p-1) = km$
  - Then $a^1 \equiv a^{1+l(p-1)} \equiv a^{km}$.
  - So $\sqrt[k]{a} \equiv \sqrt[k]{a^{km}} \equiv a^m \pmod{p}$

Ex. $\sqrt[5]{10} \mod 17$

$16 = 5 \cdot 3 + 1$

$5 = 5 \cdot 1$

$1 = 16 - 5 \cdot 3$

$1 - 16 = -5 \cdot 3$

$a^1 \equiv a^{1-16} \equiv a^{-15}$

$\sqrt[5]{a} \equiv a^{-3} \equiv a^{13}$

Thus $\sqrt[5]{10} \equiv 10^{13} \mod 17$

Try out Fermat's Little Theorem

- $3^{1000} \mod 81$

81 is not prime, so can't use FLT

- $2^{666} \mod 61$

FLT: $2^{60} \mod 61 \equiv 1$

$2^{666} \equiv 2^{6} \equiv 64 \equiv 3$

$666 \div 60 = 11$ r 6

$$\begin{array}{r} 11 \\ 60\overline{)666} \\ \underline{60} \\ 66 \\ \underline{60} \\ 6 \end{array}$$

- $\sqrt[3]{10} \mod 57$

57 is not prime

- $\sqrt[3]{10} \mod 61$

$\gcd(3, 60) = 3.$

$3^3 \equiv 27 \mod 61 \not\equiv 10$

- $\sqrt[3]{10} \mod 11$

$10^{10} \equiv 1$

$\sqrt[3]{10} \equiv \sqrt[3]{10^{11}} \equiv \sqrt[3]{10^{21}} \equiv 10^{7}$

$10^{1} \equiv 10^{1+10} \equiv 10^{21}$

$10^2 \equiv 100 \equiv 1$

$10^4 \equiv 1$

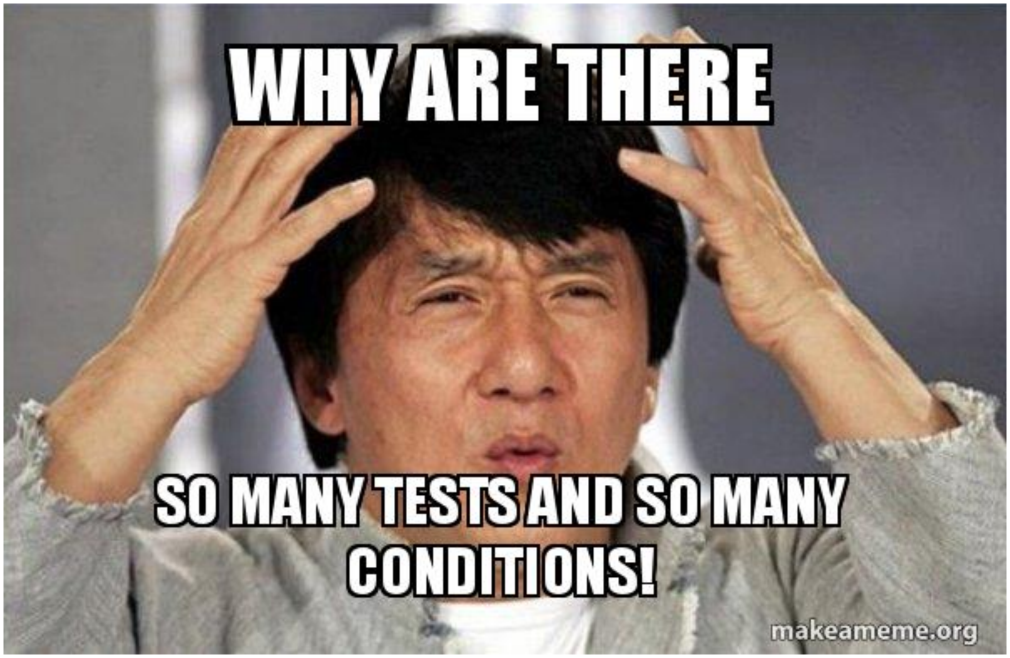
$10^7 \equiv 10^4 \cdot 10^2 \cdot 10^1$

$\equiv 10$

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

mod 7

	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

Conjecture: $a^{6n} \equiv 1$ for any n.

Conjecture: $a^{p-1} \equiv 1 \mod p$

for any prime p.

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, 4, 6, 8, 10, 12, 14
$\quad 8 \to 1,\ 10 \to 3,\ 12 \to 5,\ 14 \to 0$

$12 \equiv 5$

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

- 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.

i.e if $p=4$, then our proof won't work

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

i.e. if $a=0$ or $a=p$ or $a=2p$, then our proof won't work

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

our goal

Step 1: rewriting a^{p-1}

Because p is prime, we can divide by all numbers except 0.

And $\underbrace{\frac{a}{1} \equiv \frac{2a}{2} \equiv \frac{3a}{3} \equiv \cdots \equiv \frac{(p-1)a}{p-1}}_{p-1 \text{ ways of writing } a}$

Then $a^{p-1} \equiv \underbrace{a \cdot a \cdot a \cdots a}_{p-1 \text{ times}}$

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

Step 2: multiples are all numbers

Bean-bag tossing exp

If $\gcd(a,p)=1$, then

$\{a, 2a, 3a, 4a, \ldots\}$ is all numbers in mod p ✓

because we can write a combo

$$1 = ka + lp$$

$$\Rightarrow 1 \equiv ka \pmod{p}$$

$$2 \equiv 2ka$$

$$3 \equiv 3ka$$

$$\vdots$$

$$p-1 \equiv (p-1)ka$$

$$p \equiv pka$$

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

$0, a, 2a, \ldots, (p-1)a, pa, (p+1)a, \ldots$

is all multiples of a.

Furthermore, $pa \equiv 0 \mod p$

$(p+1)a \equiv a \mod p$

$\vdots$

So the cycle repeats after p steps.

But, we can get all p numbers in mod p.

So each cycle must contain all of them

Thus, $\{\underline{0}, a, 2a, \ldots, (p-1)a\} = \{\underline{0}, 1, \ldots, p-1\}$

as sets. $\Rightarrow \{a, 2a, \ldots, (p-1)a\} = \{1, \ldots, p-1\}$

Step 4: putting it all together

$$a^{p-1} \equiv \frac{a}{1} \cdot \frac{2a}{2} \cdot \frac{3a}{3} \cdot \ldots \cdot \frac{(p-1)a}{p-1} \quad \text{from step 1}$$

$$\equiv 1 \mod p$$

$\blacksquare$

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.