Fermat's Little Theorem
Lecture 9a: 2022-03-14

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Experimental results

- Consider arithmetic mod 7 and arithmetic mod 12.
- Powers of 1, 2, 3, 4, 5, 6 in tables.

mod 7

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

mod 12

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

Patterns to prove

- Last time we proved powers always repeat using the pigeonhole principle, and the fact that there are only a n numbers in mod n arithmetic, but an infinite number of powers.
- Patterns for today
- Do you always get 1 as a power of a non-zero number?
  - If not, when do and don't you?

- When can you not get 0 as a power of a non-zero number?

Always getting 1 as a non-zero power

- Claim: Let $x \neq 0$. Then $x^k \equiv 1 \pmod{n}$ for some $k \neq 0$.

if n is a prime number.

proof. Note that modular powers always repeat. (A)

Thus, $x^i \equiv x^j$ for some $i \neq j$. (B)

Then $1 \equiv x^{j-i}$.

Let $k = j - i \neq 0$

(cannot divide in general)

We now have $x^k \equiv 1$ for some $k \neq 0$.

(C) → works if n is prime, may not otherwise

(D)

$x^i = x^j$

$x^0 = x^{j-i}$

Which step is wrong?

Powers in prime moduli $\not\equiv 0$

1, 3, 5, 7, 1
3 5 7 1
5 7 1
0

- Claim: Let $x \not\equiv 0$ and p a prime. Then $x^m \not\equiv 0 \pmod{p}$ for any $m > 0$.

proof Suppose for contradiction that $x^m \equiv 0$ for some $m > 0$.

We can assume that m is the smallest value such that $x^m \equiv 0$.

(A) $x^5 = x^2 \cdot x^3$

We also know that $x^k \equiv 1$ for some $k > 0$.

(B)

If $m < k$, then $x^k \equiv x^m x^{k-m} \equiv 0 \cdot x^{k-m} \equiv 0$, (C)
a contradiction.

If $m > k$, then all powers $\leq k$ are nonzero. (D)
But the powers repeat after x^k, so there isn't a 0 afterwards, either, which is also a contradiction.

Thus, we've proven the claim by

Which step is wrong?

(E) proof is correct.

Fermat's little theorem

- Let p be prime.
- If $x \not\equiv 0 \pmod{p}$, then $x^{p-1} \equiv 1 \pmod{p}$.
- For any x (including 0), can say $x^p \equiv x \pmod{p}$.

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

Ex $5^{12} \mod 13 \equiv 1$

$7^{17} \mod 17 \equiv 7$

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

↓ ↓ ↓ ↓

1 3 5 0

$12 \equiv 5$

$\frac{12}{6} \equiv \frac{5}{1}$

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

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

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.

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

all the non-zero 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

Math history

- Reminder: modular arithmetic was invented in 1801 by Carl Friedrich Gauss.

Disquisitiones Arithmeticae
by Carl Friedrich Gauss in 1801

- When was Fermat's Little Theorem developed?

1640 AD

$x^{p-1} \equiv 1 \mod p$

$\Leftrightarrow$ $x^{p-1} - 1$ is divisible by p

A: Before 1800 CE
B: 1800 CE to 1900 CE
C: 1900 CE to 1950 CE
D: 1950 CE to 2000 CE
E: After 2000 CE

Pierre de Fermat

Computing powers faster

- We can use Fermat's Little Theorem to quickly reduce large powers by division with remainder.
- Let $n = m(p-1) + r$. Then $x^n \equiv x^r \pmod{p}$.

Ex. $11^{55} \pmod{19}$

$11^{55} \equiv 11^{32} \cdot 11^{16} \cdot 11^{4} \cdot 11^{2} \cdot 11 \pmod{19}$

Alternately, $11^{18} \equiv 1 \pmod{19}$

$55 = 18 \cdot 3 + 1$ (55 ÷ 18 = 3 r 1; 55 − 54 = 1)

So $11^{55} \equiv 11^{18 \cdot 3 + 1} \pmod{19}$

$\equiv 11^{18 \cdot 3} \cdot 11$

$\equiv 1^{3} \cdot 11$

$\equiv 11 \pmod{19}$

Try it out

- $6^{363} \pmod{11}$

$36 \equiv 3 \pmod{11}$

$6^{10} \equiv 1 \pmod{11}$

$6^{363} \equiv 6^{36 \cdot 10 + 3} \equiv 6^{3} \pmod{11}$

$\equiv 36 \cdot 6 \equiv 3 \cdot 6$

$\equiv 18 \equiv 7 \pmod{11}$.

$10 \overline{)363}$ r 3

- $7^{286} \pmod{13}$

A: 4
B: 5
C: 6
D: 7
E: None of the above

Alternative for finding reciprocals

- Notice that $x^{p-1} \equiv 1 \pmod{p}$.
- Therefore, $x^{p-2} \equiv \frac{1}{x} \pmod{p}$.

Try it out

- Find $\frac{1}{12} \pmod{67}$.

A: 20
B: 24
C: 28
D: 32
E: None of the above