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 $k \neq 0$.

Which step is wrong?

Powers in prime moduli $\neq 0$

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

Which step is wrong?

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

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.

- Now we write x in $p - 1$ different ways:
  $x \equiv \frac{x}{1} \equiv \frac{2x}{2} \equiv \frac{3x}{3} \equiv \cdots \equiv \frac{(p-1)x}{p-1}$.

- Multiplying them all together gives the proof.
  $x^{p-1} \equiv \frac{x}{1}\frac{2x}{2}\frac{3x}{3}\cdots\frac{(p-1)x}{p-1} \equiv 1$

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?

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 $x^n \equiv x^r \pmod{p}$.

Try it out

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

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

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