Modular power patterns & Fermat's little theorem
Lecture 8d: 2022-03-06

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Think like a mathematician

- What are some questions you as a mathematician might be asking now about powers in modular arithmetic?

Answers in chat

- Remember when we were learning about prime numbers, a big question was prime patterns.
- We can ask similar questions here: what patterns are there in powers in modular arithmetic?
- Can 0 be a power of a non-zero number?
  - Is it always?
- Do the powers repeat?
  - If so, how long before they repeat?
- Can 1 be a non-zero power of a non-zero number?
  - Is it always?

Let's experiment

- Consider arithmetic mod 7 and arithmetic mod 12.
- Write out all the 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

Let’s experiment

- Consider arithmetic mod 7 and arithmetic mod 12.
- Write out all the 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

Conjectured patterns

only if nonprime

- Can 0 be a power of a non-zero number? Yes
  - Is it always? No

A: Yes
B: No

- Do the powers repeat? Yes
  - If so, how long before they repeat?

Cycle length ≤ modulus n
because only n possible states

- Can 1 be a non-zero power of a non-zero number? Yes
  - Is it always? Yes for prime
    No for nonprime

- What's the difference in behavior between mod 7 and mod 12?
  - Why is the behavior different?

Prime 7
Nonprime 12

Modular powers always repeat

proof. Consider mod n arithmetic.

There are n distinct numbers $\{0, 1, 2, \ldots, n-1\}$

$$x^{n+1} \equiv x \cdot x^n$$

x^n ↖ depends only on previous power

Thus, if $x^i \equiv x^j$ for $i \neq j$

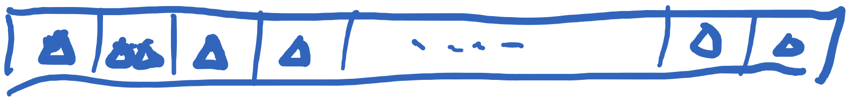
then $x^{i+1} \equiv x^{j+1}$

$x^{i+2} \equiv x^{j+2}$

$\vdots$

and so on, repetitively.

Pigeonhole principle:



$n+1$ pigeons, n boxes

$\Rightarrow$ some box has at least 2 pigeons

There are $n+1$ numbers in $\{x^0, x^1, \ldots, x^n\}$

Thus, for some $i \neq j$, $x^i \equiv x^j$,

so modular powers repeat. $\square$