Non-prime powers interactive Lecture 10b: 2022-03-23

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Beyond Fermat's Little Theorem

- For prime p, if $a \not\equiv 0 \pmod{p}$, then

can we replace p with a composite number n

what conditions do we need on a?

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

what should replace p-1

can we get a power of a congruent to 1

Non-zero power congruent to 1

- When can we get $a^t \equiv 1 \pmod{n}$?

mod 7

	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
2	2	4	1	2	4	1	2	4	1	2	4	1
3	3	2	6	4	5	1	3	2	6	4	5	1
4	4	2	1	4	2	1	4	2	1	4	2	1
5	5	4	6	2	3	1	5	4	6	2	3	1
6	6	1	6	1	6	1	6	1	6	1	6	1

Fermat's Little Thm

- Always, when n is a prime number.

What about for composite n

mod 12

	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
2	2	4	8	4	8	4	8	4	8	4	8	4
3	3	9	3	9	3	9	3	9	3	9	3	9
4	4	4	4	4	4	4	4	4	4	4	4	4
5	5	1	5	1	5	1	5	1	5	1	5	1
6	6	0	0	0	0	0	0	0	0	0	0	0

What about for composite n

mod 12

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

Only when $\gcd(a, n) = 1$

Theorem

- If $a^t \equiv 1 \pmod{n}$ for some t, then $\gcd(a, n) = 1$.

proof $a^t \equiv 1 \pmod{n}$

$\Rightarrow a^t = 1 + kn$ for some k

$\Rightarrow 1 = a^t - kn$

$\Rightarrow 1 = a \cdot a^{t-1} - k \cdot n$

So 1 is a combination of a and n.

$\Rightarrow \gcd(a, n) = 1$

(so a and n are relatively prime)

Only need tables for relative primes

mod 12

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

Only need tables for relative primes

mod 12

	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
5	5	1	5	1	5	1	5	1	5	1	5	1
7	7	1	7	1	7	1	7	1	7	1	7	1
11	11	1	11	1	11	1	11	1	11	1	11	1

- Conclusion: $a^2 \equiv 1 \pmod{12}$ for all a such that a is relatively prime to 12. That is, for all numbers a where $\gcd(a, 12) = 1$.

Powers mod 8								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1								
3								
5								
7								

Powers mod 10								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1								
3								
7								
9								

Powers mod 14								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1								
3								
5								
9								
11								
13								

Powers mod 15								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1								
2								
4								
7								
8								
11								
13								
14								

Powers mod 18								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1								
5								
7								
11								
13								
17								

Powers mod 8								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	1	1	1	1	1	1	1
3	3	1	3	1	3	1	3	1
5	5	1	5	1	5	1	5	1
7	7	1	7	1	7	1	7	1

Powers mod 10								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	1	1	1	1	1	1	1
3	3	9	7	1	3	9	7	1
7	7	9	3	1	7	9	3	1
9	9	1	9	1	9	1	9	1

Powers mod 14								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	1	1	1	1	1	1	1
3	3	9	13	11	5	1	3	9
5	5	11	13	9	3	1	5	11
9	9	11	1	9	11	1	9	11
11	11	9	1	11	9	1	11	9
13	13	1	13	1	13	1	13	1

Powers mod 15								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	1	1	1	1	1	1	1
2	2	4	8	1	2	4	8	1
4	4	1	4	1	4	1	4	1
7	7	4	13	1	7	4	13	1
8	8	4	2	1	8	4	2	1
11	11	1	11	1	11	1	11	1
13	13	4	7	1	13	4	7	1
14	14	1	14	1	14	1	14	1

Powers mod 18								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	1	1	1	1	1	1	1
5	5	7	17	13	11	1	5	7
7	7	13	1	7	13	1	7	13
11	11	13	17	7	5	1	11	13
13	13	7	1	13	7	1	13	7
17	17	1	17	1	17	1	17	1

Patterns from exercise

- Can you conjecture any patterns from which columns were all ones?

$a^2 \equiv 1 \mod 8$

$a^4 \equiv 1 \mod 10$

$a^6 \equiv 1 \mod 14$

$a^4 \equiv 1 \mod 15$

$a^6 \equiv 1 \mod 18$

- Does it help if you include prime modulus?

$a^2 \equiv 1 \mod 3$

$a^4 \equiv 1 \mod 5$

$a^6 \equiv 1 \mod 7$