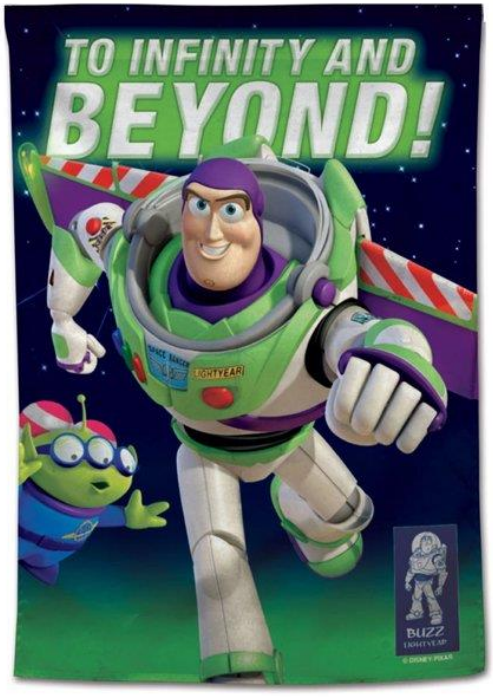
Modular powers & Successive squaring Lecture 8c: 2022-03-06

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

What are exponents?

- Exponents are repeated multiplication.
- In the ordinary integers, powers get big, super fast.



- In modular arithmetic, powers bounce around the circle.

How many steps to compute?

- How many times do you have to multiply to figure out 2^{16}?

A: 4
B: 8
C: 15
D: 16
E: None of the above

Method of successive squaring

- For any x^n, if n is a power of 2, we can quickly compute it by repeatedly squaring.

- If n is not a power of 2, we can rewrite it as a sum of powers of 2, and then multiply them together.

- To break up the exponent into a sum of powers of 2, we repeatedly subtract the largest power of 2 that's smaller than the remaining piece.

Try it out

- Compute $7^{42} \pmod{11}$

$$2^0 = 1$$
$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 8$$
$$2^4 = 16$$
$$2^5 = 32$$
$$2^6 = 64$$
$$2^7 = 128$$
$$2^8 = 256$$
$$2^9 = 512$$
$$2^{10} = 1024$$

A: 1
B: 3
C: 5
D: 7
E: None of the above

Try it out

- Compute $11^{55} \pmod{19}$

$$2^0 = 1$$
$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 8$$
$$2^4 = 16$$
$$2^5 = 32$$
$$2^6 = 64$$
$$2^7 = 128$$
$$2^8 = 256$$
$$2^9 = 512$$
$$2^{10} = 1024$$

A: 3
B: 7
C: 11
D: 15
E: None of the above

Try it out in modular arithmetic

- Compute $3^{1300} \pmod{100}$

$$2^0 = 1$$
$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 8$$
$$2^4 = 16$$
$$2^5 = 32$$
$$2^6 = 64$$
$$2^7 = 128$$
$$2^8 = 256$$
$$2^9 = 512$$
$$2^{10} = 1024$$

A: 1
B: 50
C: 81
D: 89
E: None of the above