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

MAT A02 – Winter 2022 – UTSC

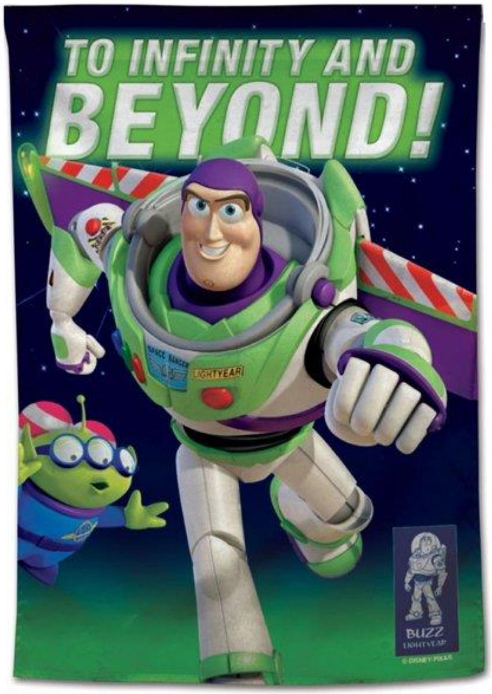
Prof. Yun William Yu

What are exponents?

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

1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, ...

1, 3, 9, 27, 81, 243, 829, ...



- In modular arithmetic, powers bounce around the circle.

In base 12:

1, 2, 4, 8, 4, 8, 4, 8, 4, 8, ...

1, 3, 9, 3, 9, 3, 9, 3, 9, ...

How many steps to compute?

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

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \; \} \; 15 \text{ multiplications}$$

$$\underbrace{2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2}_{2^8} \cdot \underbrace{2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2}_{2^8}$$

7 multiplications to get 2^8

1 multiplication to ~~get~~ $2^8 \cdot 2^8$

} 8 multi.

$$(((2^2)^2)^2)^2$$

$2^2 = 2 \cdot 2$

$2^4 = 2^2 \cdot 2^2$

$2^8 = 2^4 \cdot 2^4$

$2^{16} = 2^8 \cdot 2^8$

} 4 multipl.

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.

$3^2 \to 3^4 \to 3^8 \to 3^{16} \to 3^{32} \to \dots$

Aside: uses $\log_2 n$ multiplications

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

3^{23}

$23 = 16 + 4 + 2 + 1$

$3^{23} = 3^{16} \cdot 3^4 \cdot 3^2 \cdot 3^1$

- 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.

$23 - \underline{16} = 7 \quad 7 - \underline{4} = 3 \quad 3 - \underline{2} = \underline{1}$

Try it out

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

$$\begin{array}{r} 42 \\ -32 \\ \hline 10 \\ -8 \\ \hline 2 \end{array}$$

$$7^{42} \equiv 7^{32} \cdot 7^{8} \cdot 7^{2}$$
$$\equiv 5 \cdot 9 \cdot 5$$
$$\equiv 25 \cdot 9 \equiv 3 \cdot 9$$
$$\equiv 27$$
$$\equiv 5$$

$$7 \equiv 7$$
$$7^2 \equiv 49 \equiv 5$$
$$7^4 \equiv 25 \equiv 3$$
$$7^8 \equiv 9$$
$$7^{16} \equiv 81 \equiv 4$$
$$7^{32} \equiv 5$$

$$\begin{array}{r} 42 \\ -16 \\ \hline 26 \\ -16 \\ \hline 10 \\ -8 \\ \hline 2 \end{array}$$

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

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

Try it out

$55 = 32 + 16 + 4 + 2 + 1$

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

$$\begin{array}{r} 55 \\ -32 \\ \hline 23 \\ -16 \\ \hline 7 \\ -4 \\ \hline 3 \\ -2 \\ \hline 1 \end{array}$$

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

$\equiv 7 \cdot 11 \cdot 11 \cdot 7 \cdot 11$

$\equiv 7^2 \cdot 11^3$

$\equiv 11^4 \equiv 11$

$11 \equiv 11$

$11^2 \equiv 121 \equiv 7$

$11^4 \equiv (11^2)^2 \equiv 7^2 \equiv 49 \equiv 11$

$11^8 \equiv 11^2 \equiv 7$

$11^{16} \equiv 11$

$11^{32} \equiv 7$

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

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

Try it out in modular arithmetic

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

$$\begin{array}{r} 1300 \\ -1024 \\ \hline 276 \\ -256 \\ \hline 20 \\ -16 \\ \hline 4 \end{array}$$

$$3^{1300} \equiv 3^{1024} \cdot 3^{256} \cdot 3^{16} \cdot 3^{4}$$
$$\equiv 81 \cdot 21 \cdot 21 \cdot 81$$
$$\equiv 61 \cdot 41$$
$$\equiv 2501 \equiv 1$$

$3^1 \equiv 3$
$3^2 \equiv 9$
$3^4 \equiv 81$
$3^8 \equiv 6561 \equiv 61$
$3^{16} \equiv 3721 \equiv 21$
$3^{32} \equiv 441 \equiv 41$
$3^{64} \equiv 1681 \equiv 81$
$3^{128} \equiv 61$
$3^{256} \equiv 21$
$3^{512} \equiv 41$
$3^{1024} \equiv 81$

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

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