Modular Exponentiation

Monday, February 23, 2026 9:35 PM

Recall: FLT

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

1] Exer

① $16^{51} \pmod 7$

$$\equiv 2^{51} \equiv (2^6)^8 \cdot 2^3 \equiv 8 \equiv 1 \pmod 7$$

Result: $b^e \pmod p$

mod p / mod (p−1)

$b^{e'}$

② $234^{23} \pmod{11}$

mod 11 / mod 10

$$\equiv 3^3 \equiv 27 \equiv 5 \pmod{11}$$

③ $234431^{44} \pmod{11}$

mod 10

$$\equiv (-1)^4 \equiv 1 \pmod{11}$$

④ $2^{49} \pmod{15}$

X 15 is not prime

$$\equiv 2^4 \equiv 2^6 \cdot 2 \equiv 4 \cdot 2 \equiv 8 \pmod{15}$$

2] Modular Exponentration

To compute $b^n \pmod m$

Alg: b, n, m

Let $n = (a_{k-1}\ a_{k-2} \cdots a_1\ a_0)_2$ ⟵

Let $x = 1$; $p = b \pmod m$;

For $i = 0$ to $k-1$

if $(a_i = 1)$ then

$x = x \cdot p \pmod m$;

$p = p * p$;

Return x

e.g. $3^{19} \pmod{11}$

$19 = 10011$

$3^{19} \pmod{11}$

$3 \longrightarrow 3^1$ ✓

$\downarrow 3^2 \longrightarrow 3^2$ ✓

$\downarrow 3^4$ ✗

$\downarrow 3^8$ ✗

$\downarrow 3^{16} \longrightarrow 3^{16}$ ✓

$\therefore 3^1 \cdot 3^2 \cdot 3^{16} = 3^{19}$

a_i	$x = 1$	$p = 3$
1	3	9
1	$27 \equiv 5$	$81 \equiv 4$
0	5	$16 \equiv 5$
0	5	$25 \equiv 3$
1	$15 \equiv 4$	9

$\therefore 3^{19} \equiv 4 \pmod{11}$

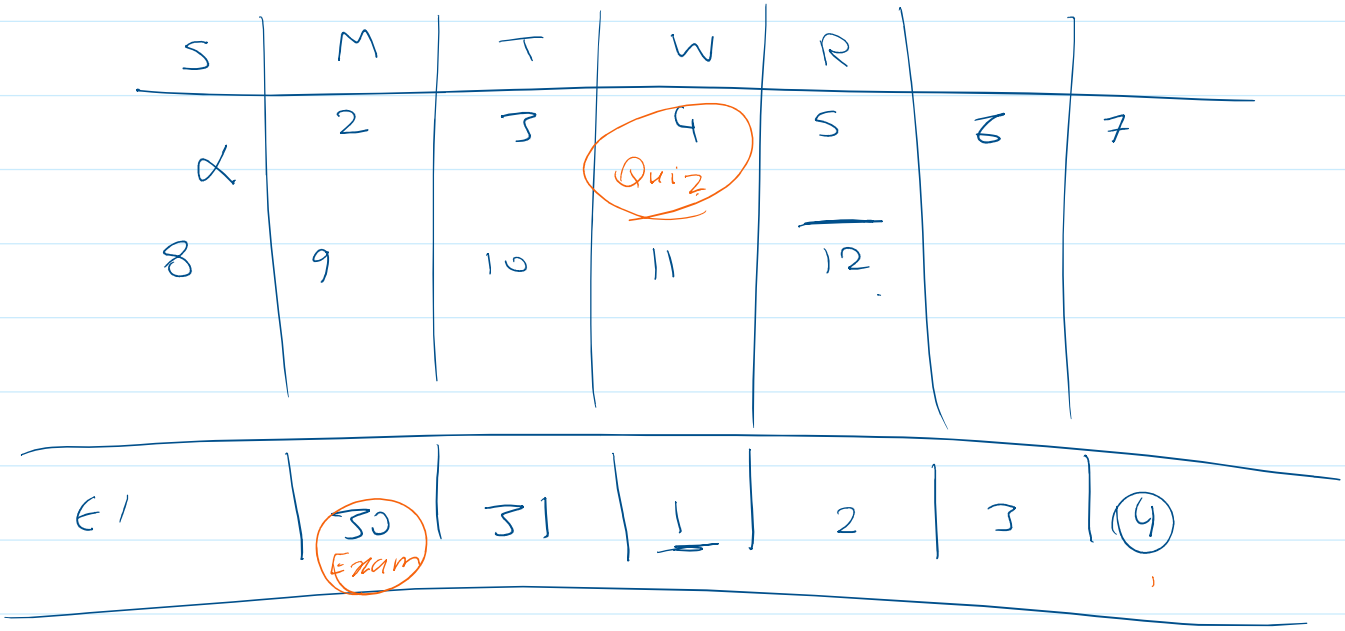
3] Time complexity:

It does at most $2 \cdot \lceil \log m \rceil$ multiplications

and at least $\lceil \log m \rceil$ multiplications

∴ time complexity is $O(n)$

Midter Exam Date March 30th


S
M
T
W
R
2
3
4
5
6
7
Quiz
8
9
10
11
12
30
Exam
31
1
2
3
4