Fast modular exponentiation

Based on marriage of 3 ideas:

1. Insertion of mod operation into any convenient add / multiply

$$(37)(63) \bmod 5 = (37 \bmod 5)(63 \bmod 5) \bmod 5$$
$$= (2)(3) \bmod 5 = 6 \bmod 5 = 1.$$

2. Shared squaring: $3^4 \cdot 2^2 = (3^2 \cdot 2)^2$

3. Every integer is writeable in binary

$$\underline{59} = 2^5 + \underline{27}$$
$$= 2^5 + 2^4 + 11$$
$$= 2^5 + 2^4 + 2^3 + 3$$
$$= \underline{2^5 + 2^4 + 2^3 + 2^1 + 2^0} = \underline{(111011)_2}$$

$$7 = (111)_2 = 2^2 + 2^1 + 2^0$$

Simple example

$$11^7 \bmod 15 = 11^{2^2+2+1} \bmod 15 = (\underline{11^2}) \cdot \underline{11^2} \cdot 11 \bmod 15$$
$$= (11^2 \cdot 11)^2 \cdot 11 \bmod 15$$
$$= \Big(\underbrace{(11^2 \bmod 15)}_{\substack{121 \bmod 15 \\ = 1}} \cdot \underbrace{(11 \bmod 15)}_{\substack{\text{extraneous,} \\ \text{no effect}}}\Big)^2 \cdot 11 \bmod 15$$
$$= (1 \cdot \underline{11})^2 \cdot 11 \bmod 15$$
$$= (11^2 \bmod 15) \cdot 11 \bmod 15$$
$$= 1 \cdot 11 \bmod 15 = \boxed{11}$$

11 ^ 7 ÷ 15

~~whole num.~~ decimal

(decimal)(15) = ans

"Fast"? Modular Exponentiation

See Rosen 4.2

(Cherry pick this concept, skim others)

Example: $66^{59} \bmod 7 = (\underline{66} \bmod 7)^{59} \bmod 7$

$= 3^{59} \bmod 7$

$$3^{59} \bmod 7 = 3^{(111011)_2} \bmod 7$$

$$= 3^{2^5+2^4+2^3+2+1} \bmod 7$$

$$= 3^{2^5} \cdot 3^{2^4} \cdot 3^{2^3} \cdot 3^{2} \cdot 3 \bmod 7$$

$$= \left[3^{2^4} \cdot 3^{2^3} \cdot 3^{2^2} \cdot 3\right]^2 \cdot 3 \bmod 7$$

$$= \left[\left[3^{2^3} \cdot 3^{2^2} \cdot 3^{2}\right]^2 \cdot 3\right]^2 \cdot 3 \bmod 7$$

$$= \left[\left[\left[3^{2^2} \cdot 3^{2} \cdot 3\right]^2\right]^2 \cdot 3\right]^2 \cdot 3 \bmod 7$$

$$= \left[\left[\left[\left[3^2 \cdot 3\right]^2 \cdot 3\right]^2\right]^2 \cdot 3\right]^2 \cdot 3 \bmod 7$$

$$= \left[\left[\left[\left[(3^2 \bmod 7) \cdot 3\right]^2 \cdot 3\right]^2\right]^2 \cdot 3\right]^2 \cdot 3 \bmod 7$$

$$= \left[\left[\left[\underbrace{\left(\left[2 \cdot 3\right]^2 \bmod 7\right) \cdot 3}_{=1 \cdot 3}\right]^2\right]^2 \cdot 3\right]^2 \cdot 3 \bmod 7$$

$$= \left[\left[(3)^2\right]^2 \cdot 3\right]^2 \cdot 3 \bmod 7$$

$$= \left[\left[3^2 \bmod 7\right]^2 \cdot 3\right]^2 \cdot 3 \bmod 7$$

$$= \left[2^2 \cdot 3\right]^2 \cdot 3 \bmod 7$$

$$= \left[2^2 \cdot 3 \bmod 7\right]^2 \cdot 3 \bmod 7$$

$$= [5]^2 \cdot 3 \mod 7$$

$$= (\underbrace{5^2 \mod 7}_{=4}) \cdot 3 \mod 7$$

$$= 12 \mod 7$$

$$= \boxed{5.}$$

Suggestion: You try this (make up your own, or try)

$41^{18} \mod 59$

$37^{71} \mod 4$

can check using app

$$\underline{3}^{17} \mod \underline{80} = (3^4)^4 \cdot 3 \mod 80 = (81 \mod 80)^4 \cdot 3 \mod 80$$

if you notice this

$$= \underline{1} \cdot 3 \mod 80$$

$$= \underline{3}$$

Thus,

$$
\begin{aligned}
87^{109} \bmod 4501 &= 87^{64+32+8+4+1} \bmod 4501 \qquad \text{(Idea \#1)} \\
&= (87)^{64}(87)^{32}(87)^{8}(87)^{4}(87) \bmod 4501 \qquad \text{(algebra)} \\
&= (((((87^2)^2)^2)^2)^2)^2((((87^2)^2)^2)^2)^2((87^2)^2)^2(87^2)^2(87) \bmod 4501 \qquad \text{(algebra)} \\
&= [((((87^2)^2)^2)^2)^2 \cdot (((87^2)^2)^2)^2 \cdot (87^2)^2 \cdot 87^2]^2(87) \bmod 4501 \qquad \text{(Idea \#3)} \\
&= [[(((87^2)^2)^2)^2 \cdot ((87^2)^2)^2 \cdot 87^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#3)} \\
&= [[[((87^2)^2)^2 \cdot (87^2)^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#3)} \\
&= [[[[(87^2)^2 \cdot 87^2]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#3)} \\
&= [[[[[87^2 \cdot 87]^2]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#3)} \\
&= [[[[[(87^2 \bmod 4501) \cdot 87]^2]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)} \\
&= [[[[[3068 \cdot 87]^2]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(since } 87^2 \bmod 4501 = 3068\text{)} \\
&= [[[[[3068 \cdot 87 \bmod 4501]^2]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)} \\
&= [[[[1357^2]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(since } 3068 \cdot 87 \bmod 4501 = 1357\text{)} \\
&= [[[[1357^2 \bmod 4501]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)} \\
&= [[[540^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(since } 1357^2 \bmod 4501 = 540\text{)} \\
&= [[[(540^2 \bmod 4501) \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)} \\
&= [[[3536 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(since } 540^2 \bmod 4501 = 3536\text{)} \\
&= [[[3536 \cdot 87 \bmod 4501]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)} \\
&= [[1564^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(since } 3536 \cdot 87 \bmod 4501 = 1564\text{)} \\
&= [[(1564^2 \bmod 4501) \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)} \\
&= [[2053 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(since } 1564^2 \bmod 4501 = 2053\text{)} \\
&= [[2053 \cdot 87 \bmod 4501]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)} \\
&= [3072^2]^2(87) \bmod 4501 \qquad \text{(since } 2053 \cdot 87 \bmod 4501 = 3072\text{)} \\
&= [3072^2 \bmod 4501]^2(87) \bmod 4501 \qquad \text{(Idea \#2)} \\
&= 3088^2(87) \bmod 4501 \qquad \text{(since } 3072^2 \bmod 4501 = 3088\text{)} \\
&= (3088^2 \bmod 4501)(87) \bmod 4501 \qquad \text{(Idea \#2)} \\
&= (2626)(87) \bmod 4501 \qquad \text{(since } 3088^2 \bmod 4501 = 2626\text{)} \\
&= 3412.
\end{aligned}
$$

Monday: Introduced congruence/equivalence mod m

$$a \equiv b \pmod{m} \quad \text{iff} \quad m \mid a-b$$

Note: fix modulus $m = 5$

$\mathbb{Z}$: $\ldots, -11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6 \ldots$

is equivalent (in mod 5) to

0: $\ldots, -20, -15, -10, -5, 0, 5, 10, \ldots$

1: $\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots$

2: $\ldots, -8, -3, 2, 7, 12, \ldots$

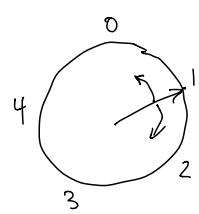
3: $\ldots, -7, -2, 3, 8, 13, \ldots$

4: $\ldots, -6, -1, 4, 9, 14, \ldots$

5:

5 representatives (the 5 remainders possible when $\div 5$) for integers mod 5

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$



$$\mathbb{Z}_3 = \{0, 1, 2\}$$

modulus