**Fast Modular Exponentiation is based on these three ideas:**

**Idea #1**: Every positive integer can be written as sums of powers of 2.

The powers of two are

$$\begin{array}{lll} 2^0 = 1 & 2^4 = 16 & 2^8 = 256 \\ 2^1 = 2 & 2^4 = 32 & 2^9 = 512 \\ 2^2 = 4 & 2^4 = 64 & 2^{10} = 1024 \\ 2^3 = 8 & 2^4 = 128 & 2^{11} = 2048 \end{array}$$

and so on. We can write the integers as sums of these powers

$$\begin{array}{lcl} 1 & = & 2^0 \\ 2 & = & 2^1 \\ 3 & = & 1+2 = 2^0+2^1 \\ 4 & = & 2^2 \\ 5 & = & 4+1 = 2^2+2^0 \\ 6 & = & 4+2 = 2^2+2^1 \\ 7 & = & 4+2+1 = 2^2+2^1+2^0 \\ 8 & = & 2^3 \\ \vdots & & \end{array} \qquad \begin{array}{lcl} 63 & = & 32+16+8+4+2+1 = 2^5+2^4+2^3+2^2+2^1+2^0 \\ 64 & = & 2^6 \\ 65 & = & 64+1 = 2^6+2^0 \\ \vdots & & \\ 254 & = & 2^7+2^6+2^5+2^4+2^3+2^2+2^1 \\ 255 & = & 2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0 \\ 256 & = & 2^8 \\ 257 & = & 256+1 = 2^8+2^0 \\ \vdots & & \end{array}$$

**Idea #2**: Arithmetic operations in mod $n$ allow you to "mod" along the way.

$(27)(33) \bmod 8$ is the same as $(27 \bmod 8)(33 \bmod 8) \bmod 8 = (3)(1) \bmod 8 = 3.$
$(27+33) \bmod 8$ is the same as $((27 \bmod 8) + (33 \bmod 8)) \bmod 8 = (3+1) \bmod 8 = 4.$
$10^{15} \bmod 13$ is the same as

$$\begin{aligned} (5\cdot 2)^{15} \bmod 13 &= (5^{14})(5)(2^{12})(2^3) \bmod 13 = (5^2)^7(5)(2^6)^2(2^3) \bmod 13 \\ &= (-1)^7(5)(-1)^2(2^3) \bmod 13 = (-1)(40) \bmod 13 \\ &= (-1)(40 \bmod 13) \bmod 13 = (-1) \bmod 13 = 12. \end{aligned}$$

**Idea #3**: Combined squaring

We have

$$\begin{aligned} &(7^2)(5^2) \bmod 11 = (7\cdot 5)^2 \bmod 11 = 2^2 \bmod 11 = 4, \text{ and} \\ &(31^8)(7^2) \bmod 55 = [(31^2)^2]^2(7^2) \bmod 55 = [(31^2)^2 \cdot 7]^2 \bmod 55 \\ &\qquad = [(31^2 \bmod 55)^2 \cdot 7]^2 \bmod 55 = [(26)^2 \cdot 7]^2 \bmod 55 \\ &\qquad = [(26^2 \bmod 55) \cdot 7]^2 \bmod 55 = (16\cdot 7)^2 \bmod 55 = 2. \end{aligned}$$

Fast modular exponentiation is the result of combining Ideas #1–#3. For instance, when raising $37^{109} \bmod 4501$, we can first use Idea #1 to write the *exponent*

$$109 \;=\; 64+32+8+4+1 \;=\; 2^6+2^5+2^3+2^2+2^0.$$

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) \\
&= [[[[[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) \\
&= [[[[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) \\
&= [[[(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) \\
&= [[[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) \\
&= [[(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) \\
&= [[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) \\
&= [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) \\
&= (3088^2 \bmod 4501)(87) \bmod 4501 \qquad \text{(Idea \#2)} \\
&= (2626)(87) \bmod 4501 \qquad (\text{since } 3088^2 \bmod 4501 = 2626) \\
&= 3412.
\end{aligned}
$$