Example: $3^x \equiv 26 \pmod{127}$

$N = 126 = 2 \cdot 3^2 \cdot 7$

(a) For $x \bmod 2$: $x \equiv 0 \pmod 2$

1b) For $x \bmod 7$:

We raise to the power $\frac{126}{7} = 18$

$3^{18} \equiv 4,\ 26^{18} \equiv 8 \pmod{127}$

$4^x \equiv 8 \pmod{127}$

$4^0 \equiv 1,\ 4^1 \equiv 4,\ 4^2 \equiv 16,\ 4^3 \equiv 64,\ 4^4 \equiv 2,\ 4^5 \equiv 8 \pmod{127}$

$\Rightarrow x \equiv 5 \pmod 7$.

1c) For $x \bmod 9$:

Raise to the power $\frac{126}{9} = 14$

$3^{14} \equiv 22,\ 26^{14} \equiv 68 \pmod{127}$

$22^x \equiv 68 \pmod{127}$

$22^0 \equiv 1,\ 22^1 \equiv 22,\ 22^2 \equiv 103,\ 22^3 \equiv 107,\ 22^4 \equiv 68 \pmod{127}$

$\Rightarrow x \equiv 4 \pmod 9$.

1d) We have $\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 5 \pmod 7 \\ x \equiv 4 \pmod 9 \end{cases}$

Start with last two congruencies:

$1 = 7 \cdot 4 - 9 \cdot 3$

Then $x \equiv 4 \cdot 7 \cdot 4 - 5 \cdot 9 \cdot 3 = -23 \equiv 40 \pmod{63}$.

Add $x \equiv 0 \pmod 2$

Finally: $x \equiv 40 \pmod{126} \Rightarrow \log_{3,127}(26) = 40$.

One more idea: To compute $x \pmod{q^k}$ we can firstly compute $x \pmod q$ then $x \pmod{q^2}$, ..., $x \pmod{q^k}$.

Note: Number x written in base q is

$$x = (d_m d_{m-1} \dots d_1 d_0)_q \qquad d_i \in \{0, 1, \dots, q-1\}$$
$$= d_m \cdot q^m + d_{m-1} q^{m-1} + \dots + d_1 q + d_0.$$

Then the residue of $x \pmod{q^i}$ is

$\cancel{(q_{i-1} \dots q_1 q_0)_q}$.

$(d_{i-1} \dots d_1 d_0)_q$.

Hence, given $x \pmod{q^i}$ there are q possibilities for $x \pmod{q^{i+1}}$.

Example: $3^x \equiv 5 \pmod{17}$. $N = 16 = 2^4$.

(a) Find $x \pmod 2$.

Raise both sides to the power 8.

$3^2 \equiv 9,\ 3^4 \equiv 13,\ 3^8 \equiv 16 \pmod{17}$

$5^2 \equiv 8,\ 5^4 \equiv 13,\ 5^8 \equiv 16 \pmod{17}$

$16^x \equiv 16 \pmod{17} \Rightarrow x \equiv 1 \pmod 2$

(b) Find $x \pmod 4$

$(x \equiv 1 \text{ or } 3 \pmod 4)$

$(3^4)^x \equiv 5^4 \pmod{17}$

$13^x \equiv 13 \pmod{17} \Rightarrow x \equiv 1 \pmod 4$

(c) Find $x \pmod 8$

$(x \equiv 1 \text{ or } 5 \pmod 8)$

$9^x \equiv 8 \pmod{17} \Rightarrow x \equiv 5 \pmod 8$

1d) Find x itself.

$(x = 5 \text{ or } 13)$

$3^5 \equiv 5 \pmod{17} \Rightarrow x = 5.$

In general, let q^k be a prime power from the factorization of N.

To compute $x \pmod{q^k}$ we compute the sequence $x_0, x_1, x_2, \dots, x_k$, where $x_i \equiv x \pmod{q^i}$.

$x_0 = 1.$

If we have x_i then $x_{i+1} = y \cdot q^i + x_i$, $y \in \{0, \dots, q-1\}$

$$\left(b^{\frac{N}{q^{i+1}}}\right)^{x_{i+1}} \equiv a^{\frac{N}{q^{i+1}}} \pmod{p}$$

$$\Leftrightarrow \left(b^{\frac{N}{q^{i+1}}}\right)^{y \cdot q^i + x_i} \equiv a^{\frac{N}{q^{i+1}}} \pmod{p}$$

$$\Leftrightarrow \left(b^{\frac{N}{q}}\right)^{y} \equiv \left(b^{\frac{N}{q^{i+1}}}\right)^{-x_i} \cdot a^{\frac{N}{q^{i+1}}} \pmod{p}$$

This is anothe DLP with the order q.
We either use naive approach or Baby-step/Giant-step to solve it in $O(q)$ or $O(\sqrt{q})$ modular operations.

In total, DLP of order $N = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$ can be transformed into α_1 DLP's of order q_1, α_2 DLP's of orde q_2, ..., α_r DLP's of order q_r.

Note: We have no improvement if $N = q$ is prime, have very little improvement if $N = 2q$ (for safe primes).

Example: $2^x \equiv 14 \pmod{19}$. $N = 18 = 2 \cdot 3^2$.

Should find x mod 2, mod 9.

(1a) Find $x \pmod 9$.

Start with $x \pmod 3$

$(2^6)^x \equiv 14^6 \pmod{19}$.

$7^x \equiv 7 \pmod{19} \Rightarrow x \equiv 1 \pmod 3$.

Continue with $x \pmod 9$.

$x \equiv 3y+1 \pmod 9$, $y \in \{0, 1, 2\}$.

$(2^2)^x \equiv 14^2 \pmod{19}$

$4^{3y+1} \equiv 6 \pmod{19}$

$(4^3)^y \equiv 4^{-1} \cdot 6 \pmod{19}$

$7^y \equiv 11 \pmod{19} \Rightarrow y = 2$

$x \equiv 7 \pmod 9$.

(1b) Find $x \pmod 2$.

Complete this example - Ex.