Find the discrete logarithm of $y = 39$ to the base 2 in $F_{101}$.

```
with(numtheory):
p := 101 : isprime(p);
    true

b := 2 : n := order(b, p) : ifactor(n);
(2) (5) 2

Thus, $n = \text{ord}(2) = 100 = 2^2 5^2$.

1. Precomputations:

Case 1: $p_1 = 2$:

```
p1 := 2 : cl := modp(b^{p1}, p);
c1 := 100
```

```
pt1 := [1, cl] : lt1 := [[1, 0], [100, 1]];
lt1 := [[1, 0], [100, 1]]
```

Note: $pt1$ is the power table of $c_1$, so its $i$-th entry is $c_1^{i-1}$. Since $p_1 = 2$, its length is 2.
Moreover, $lt1$ is the log table of $\langle c_1 \rangle = pt1 = \{1, 100\}$ to the base $c_1$.

Case 2: $p_2 = 5$:

```
p2 := 5 : c2 := modp(b^{p2}, p);
c2 := 95
```

```
pt2 := [ seq(modp(c2^i, p), i = 0..4 ) ];
pt2 := [1, 95, 36, 87, 84]
```

```
l t1 := [[1, 0], [26, 2], [84, 4], [87, 3], [95, 1]];
lt1 := [[1, 0], [26, 2], [84, 4], [87, 3], [95, 1]]
```

Note: $pt2$ is the power table of $c_2$, so its $i$-th entry is $c_2^{i-1}$. Since $p_2 = 5$, its length is 5.
Moreover, $lt2$ is the log table of $\langle c_2 \rangle = pt2 = \{1, 26, 84, 87, 95\}$ to the base $c_2$.

2. Apply SPH to find $DL_b(y)$ for $y = 39$.

```
y := 39 :
```

Case 1: $p_1 = 2$, $\alpha_1 = 2$:

```
y0 := y : x0 := modp(y0^{p1}, p);
x0 := 100
```

Thus, using the above power table $pt1$ (or the log table $lt1$) we see that $x_0 = DL_{c_1}(X_0) = DL_{100}(100) = 1$.

```
x0 := 1 : y1 := modp(y0^{p1}, p); X1 := modp(y1^{p2}, p);
y1 := 70
X1 := 100
```

Thus, using the above power table $pt1$ we see that $x_1 = DL_{c_1}(X_1) = DL_{100}(100) = 1$,
and so $x = x_0 + 2^1 x_1 = 3 \mod 4$. 

```
```
Case 2: $p_2 = 5$, $\alpha_2 = 2$:

\[ y_0 := y : X_0 := \text{modp}\left(\frac{n}{y_0 \cdot p_2^2}, p\right); \]
\[ X_0 := 1 \]  

Thus, using the above power table $pt_2$ we see that
\[ x_0 = \text{DL}_c(X_0) = \text{DL}_{95}(1) = 0. \]

\[ x_0 := 0 : y_1 := \text{modp}\left(\frac{y_0}{b^{x_0}}, p\right); X_1 := \text{modp}\left(y_1 \cdot p_2^2, p\right); \]
\[ y_1 := 39 \]
\[ X_1 := 36 \]

Thus, using the above power table $pt_2$ we see that
\[ x_1 = \text{DL}_c(X_1) = \text{DL}_{95}(36) = 2, \]
and so $x = x_0 + 5 \cdot x_1 = 10 \pmod{25}$.

**Conclusion: apply CRT.**

By Cases 1 and 2 we have $x \equiv 3 \pmod{4}$ and $x \equiv 10 \pmod{25}$

\[ \text{chrem([3, 10], [4, 25]);} \]
\[ 35 \]

Note the chrem( ) is Maple's CRT. Thus, $\text{DL}_b(y) = 35$. Check this:

\[ \text{evalb(modp}(b^{35}, p) = y); \]
\[ \text{true} \]

**Note:** In the above computation we had computed the discrete log "by inspection".

However, by using Maple's "member" command, we can let MAPLE do this table look-up for us. This is done by the following a Maple program.


\[ \text{DL} := \text{proc}(y, pt) \text{ local } p; \]
\[ \text{member}(y, pt, 'p'); \]
\[ \text{return}(p - 1); \text{ end;}; \]

Test this for the above values $pt = pt_2$, $y = X_1$

\[ \text{DL}(X_1, pt_2); \]
\[ 2 \]

This agrees with what we had above.