

To Solve " $2^x \bmod 107 = 6$ "

p	107
n = order	106

m	11	
a	6	
g	2	h 54

i	1	2	3	4	5	6	7	8	9	10
h^i	54	27	67	87	97	102	51	79	93	100
ah^i	3	55	81	94	47	77	92	46	23	65
g^{mi}	15	11	58	14	103	47	63	89	51	16

$$X = 6 * 11 + 5 = 71$$

Commands used:

```
n = 107
```

```
e_mod 2 (n-2) n
```

```
[e_mod 54 i n | i <- [1..11]]
```

```
[e_mod 2 (i * 11) n | i <- [1..11]]
```

To Solve " $2^x \bmod 107 = 6$ "

m
11
50
86
26