

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

p	107
n = order	106

m	11
a	6
g	2

h	54
---	----

	m										
i	1	2	3	4	5	6	7	8	9	10	11
h^i	54	27	67	87	97	102	51	79	93	100	50
ah^i	3	55	81	94	47	77	92	46	23	65	86
g^{mi}	15	11	58	14	103	47	63	89	51	16	26

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

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]]
```