

$$m = 7849$$

$$\sqrt{m} = 88,594\dots$$

$$b_{-1} = 1$$

$$b_0 = a_0 = 88$$

$$x_0 = \sqrt{m} - a_0 = 0,594\dots$$

$$b_0^2 \bmod m = b_0^2 - m = -105 = (-1) \times 3 \times 5 \times 7$$

$$a_1 = \left[ \frac{1}{x_0} \right] = 1$$

$$x_1 = \frac{1}{x_0} - a_1 = 1,681\dots - 1 = 0,681\dots$$

$$b_1 = a_1 b_0 + b_{-1} = 1 \times 88 + 1 = 89$$

$$b_1^2 \bmod m = 72 = 2^3 \times 3^2$$

$$a_2 = \left[ \frac{1}{x_1} \right] = 1$$

$$x_2 = \frac{1}{x_1} - a_2 = 1,466\dots - 1 = 0,466\dots$$

$$b_2 = a_2 b_1 + b_0 = 1 \times 89 + 88 = 177$$

$$b_2^2 \bmod m = -67 = (-1) \times 67$$

...

I wrote a python program that generated 24 values. This is the code :

```

import math

table = []

n = 7849
i = 0
b = [1,math.floor(math.sqrt(n))]
a = math.floor(math.sqrt(n))
x = math.sqrt(n) - a
bmn = b[1]*b[1] - n

print(i)
print(str(a) + " " + str(x) + " " + str(b[1]) + " " + str(bmn))
print("")

for i in range(20):
    a = math.floor(float(1)/x)
    x = float(1)/x - a
    lb,llb = b[1],b[0]
    b[1] = (a * lb + llb) % n
    b[0] = lb
    bmn = ( b[1]*b[1] ) % n
    if bmn > n/2:
        bmn = bmn - n
    print(i+1)
    print(str(a) + " " + str(x) + " " + str(b[1]) + " " + str(bmn))
    print("")

```

i	0	1	2	3	4	5	6	7	8	9	10
ai	88	1	1	2	6	1	58	5	21	1	18
bi	88	89	177	443	2835	3278	4583	2646	5206	3	5260
b <sup>2</sup> mod n	-105	72	-67	24	-151	3	-35	8	-161	9	-125
	$(-1)^* 3^* 5^* 7$	$2^3^* 3^2$	$(-1)^* 67$	$2^3^* 3$	$(-1)^* 151$	3	$(-1)^* 5^* 7$	$2^{**}3$	$(-1)^* 7^* 23$	$3^2$	$(-1)^* 5^3$
i	11	12	13	14	15	16	17	18	19	20	
ai	1	1	1	4	2	1	3	2	20	2	
bi	5263	2674	88	3026	6140	1317	2242	5801	527	6855	
b <sup>2</sup> mod n	48	-163	-105	-3107	853	-140	3204	2938	3014	-938	
	$2^4^* 3$	$(-1)^* 163$	$(-1)^* 3^* 5^* 7$	$(-1)^* 13^* 239$	853	$(-1)^* 2^2^* 5^* 7$	$2^2^* 3^2^* 89$	$2^* 13^* 113$	$2^* 11^* 137$	$(-1)^* 2^* 7^* 67$	

We choose  $B = \{-1, 2, 3, 5, 7\}$ . Then  $b_i^2 \pmod m$  is a B-number for  $i = 0, 1, 3, 6, 5, 7, 9, 10, 11, 13, 16$  if we generated more than 6 values)

$$v_0 = (1, 0, 1, 1, 1)$$

$$v_5 = (0, 0, 1, 0, 0)$$

$$v_1 = (0, 3, 2, 0, 0)$$

$$v_6 = (1, 0, 0, 1, 1)$$

$$v_3 = (0, 3, 1, 0, 0)$$

Then  $v_0 + v_1 + v_3 + v_6 = 0 \pmod 2$ . Hence

$$b = b_0 + b_1 + b_3 + b_6 = 88 + 89 + 443 + 4583 = 5329 \pmod m$$

$$c = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520 \neq$$

$$-c = 5329 \pmod m$$

$b = -c \pmod m$ , so we generate more values (from 6 to 20)

We choose  $B = \{-1, 2, 5, 7, 67\}$ . Then  $b_i^2 \bmod m$  is a B-number for  $i = 2, 6, 7, 10, 16, 20$

$$v_2 = (1, 0, 0, 0, 1) \quad v_{10} = (1, 0, 3, 0, 0)$$

$$v_6 = (1, 0, 1, 1, 0) \quad v_{16} = (1, 2, 1, 1, 0)$$

$$v_7 = (0, 3, 0, 0, 0) \quad v_{20} = (1, 1, 0, 1, 1)$$

Then  $v_2 + v_7 + v_{10} + v_{16} + v_{20} = 0 \pmod{2}$ . Hence

$$b = b_2 \cdot b_7 \cdot b_{10} \cdot b_{16} \cdot b_{20} = 2785 \pmod{m}$$

$$c = 2^3 \cdot 5^2 \cdot 7 \cdot 67 = 7461$$

$$-c = 388 \pmod{m}$$

$b \neq \pm c \pmod{m}$ , so a factor of  $m$  is  $(2785 + 7461, 7849) = 47$ .

$$\text{Thus, } m = 47 \cdot 167$$