

$$n = 7163$$

For Steps 1-6 I used a program that helped me compute the table:

i	0	1	2	3	4	5
$a_i$	84	1	10	1	2	1
$b_i$	84	85	169	254	677	931
$b_i \bmod n$	-107	62	-91	49	-103	38

We decompose the  $b_i^2 \bmod n$  elements so we can choose a  $B$ .

$$-107 = (-1) \cdot 107 \quad 49 = 7^2$$

$$62 = 2 \cdot 31 \quad -103 = (-1) \cdot 103$$

$$-91 = (-1) \cdot 7 \cdot 13 \quad 38 = 2 \cdot 19$$

Step 7

By analysing the decompositions in prime factors, we choose  $B$  with bases that appear in at least two decompositions and with -1

$$\text{Let } B = \{-1, 2, 7\}$$

We write for each number their associate vectors.

~~Each~~ Each vector is computed by putting the exponent mod 2 of each respective base from  $B$ .

$$-107 \Rightarrow v_0 = (1, 0, 0)$$

$$49 \Rightarrow v_3 = (0, 0, 0)$$

$$62 \Rightarrow v_1 = (0, 1, 0)$$

$$-103 \Rightarrow v_4 = (1, 0, 0)$$

$$-91 \Rightarrow v_2 = (1, 0, 1)$$

$$38 \Rightarrow v_5 = (0, 1, 0)$$

Step 10

we need to find  $b$ , which is the product of the  $b_i$ 's of which vectors yielded sum 0

$$v_0 + v_1 + v_4 + v_5 = (1, 0, 0) + (0, 1, 0) + (1, 0, 0) + (0, 1, 0) = 0$$

We also compute  $c$ , which is the product of the bases involved (without -1) to the power found in the vectors / 2

$$v_2 = \frac{1}{2}(1+1) = 1 \quad v_7 = 0$$

$$\Rightarrow c = 2^1 \cdot 7^0 = 2$$

$$\Rightarrow b = (84 \cdot 85 \cdot 677 \cdot 931) \bmod 7163 = 1311$$

Step 11  $1311 \neq 2 \bmod 7163$

$\Rightarrow (b+c, n)$  or  $(b-c, n)$  is a non-trivial factor of  $n$

$$(1313, 7163) = 13 \quad \text{and} \quad (1309, 7163) = 1$$

So, we have 13 as a non-trivial factor of 7163