Catargiu Georgiana-Ecaterina
info engleză, 932/1

Assignment B

Nr. matricol : 2491 => $n = 7987$

$i=0$: $a_0 = b_0 = [\sqrt{n}] = 89$

$b_0^2 \bmod n = 7921 = -66$

$x_0 = \sqrt{n} - a_0 = 0,3700$

$i=1$: $a_1 = \left[\frac{1}{x_0}\right] = \left[\frac{1}{0,3700}\right] = 2$

$x_1 = \frac{1}{x_0} - a_1 = 0,7027$

$b_1 = a_1 b_0 + b_{-1} = 2 \cdot 89 + 1 = 179$

$b_1^2 \bmod n = 93$

$i=2$: $a_2 = \left[\frac{1}{x_1}\right] = \frac{1}{0,7027} = 1$

$x_2 = \frac{1}{x_2} - a_2 = 0,4230$

$b_2 = a_2 \cdot b_1 + b_0 = 1 \cdot 179 + 89 = 268$

$b_2^2 \bmod n = 7928 = -59$

$i=3$: $a_3 = \left[\frac{1}{x_2}\right] = \left[\frac{1}{0,4230}\right] = 2$

$x_3 = \frac{1}{x_2} - a_3 = 0,3640$

$b_3 = a_3 b_2 + b_1 = 2 \cdot 268 + 179 = 715$

$b_3^2 \bmod n = 57$

In the same manner we compute the rest of i_x until we find a „pattern". For my number 12 iterations were needed in order to solve the problem.

All the iterations put together will be put in a table as follows:

i	0	1	2	3	4	5	6	7	8	9	10	11	12
a_i	89	2	1	2	2	1	3	5	2	59	8	9	3
b_i	89	179	268	715	1698	2413	950	7163	7289	5916	6695	2275	5533
$b_i^2 \bmod n$	-66	93	-59	57	-103	46	-31	81	-3	22	-19	49	-82

The factor base is $B = \{-1, 2, 3, 7, 11\}$ after analyzing the table.

$$\begin{cases} i_0 \Rightarrow -66 = (-1) \cdot 2 \cdot 3 \cdot 11 \\ i_1 \Rightarrow 93 = 3 \cdot 31 \\ i_7 \Rightarrow 81 = 3^4 \\ i_8 \Rightarrow -3 = (-1) \cdot 3 \\ i_9 \Rightarrow 22 = 2 \cdot 11 \\ i_{11} \Rightarrow 49 = 7^2 \\ i_{12} \Rightarrow -82 = (-1) \cdot 2 \cdot 41 \end{cases}$$

The subset of vector with the sum $0 \in \mathbb{Z}_2^4$ is:

$$\begin{cases} v_0 = (1, 1, 1, 0, 1) \\ v_7 = (0, 0, 4, 0, 0) \\ v_8 = (1, 0, 3, 0, 0) \\ v_9 = (0, 0, 0, 1, 0) \end{cases}$$

$$\overline{v_0 + v_7 + v_8 + v_9} = 0 \pmod 2$$

$$b = \prod b_i = b_0 \cdot b_7 \cdot b_8 \cdot b_9 = 89 \cdot 7163 \cdot 7289 \cdot 5916$$

$$\Rightarrow b = 1525 \pmod n$$

$$c = \prod p_j^{\gamma_j}, \text{ where } \gamma_j = \frac{1}{2} \sum k_{ij}$$

$$\Rightarrow c = 2 \cdot 11 \cdot 3^3 = 594$$

$$\left.\begin{matrix} b = 1525 \\ c = 594 \end{matrix}\right| \Rightarrow b \neq c \Rightarrow \begin{cases} \gcd(1525 + 594, 7987) \\ \gcd(1525 - 594, 7987) \end{cases}$$

$$= \left.\begin{cases} \gcd(2119, 7987) = 163 \\ \gcd(931, 7987) = 49 \end{cases}\right| \Rightarrow n = 163 \cdot 49 = 7987$$

R: 163, 49

```python
from math import sqrt


def getTable(number, iterations):
    ai = []
    bi = []
    xi = []
    square = int(sqrt(number))
    ai.append(square)
    bi.append(square)
    x0 = sqrt(number) - ai[0]
    xi.append(x0)
    for i in range(1, iterations + 1):
        ai.append(int(1 / float(xi[i - 1])))
        xi.append((1 / xi[i - 1]) - ai[i])
        if i == 1:
            bi.append((ai[i] * bi[i - 1] + 1) % number)
        else:
            bi.append((ai[i] * bi[i - 1] + bi[i - 2]) % number)

    return ai, bi


def main():
    print(getTable(7987, 12))


main()
```

```
"D:\An III\Crypto\A2\TestProgram\venv\Scripts\python.exe" "D:/An III/Crypto/A2/TestProgram/factor/factorize.py"
([89, 2, 1, 2, 2, 1, 3, 5, 2, 59, 8, 9, 3], [89, 179, 268, 715, 1698, 2413, 950, 7163, 7289, 5916, 6695, 2275, 5533])

Process finished with exit code 0
```