28 Подвесить сервер

Задача. При изучении программ поискового сервера Moctod Виктор нашел объявление переменной `a`:

```
unsigned a = 1;
```

Виктор выяснил, что эта переменная меняется только при обработке двух специальных поисковых запросов. При обработке запроса `"Ring ring ring"` переменная преобразуется следующим образом:

```
a = a / 2 ^ (a % 2) * 96;
```

а при обработке запроса `"In the finite field"` немного по-другому:

```
a ^= a / 2 ^ (a % 2) * 96;
```

Как только переменная `a` снова принимает значение 1 сервер зависает. Сможет ли Виктор подвесить сервер, выполнив 18 запросов? 19 запросов?

Решение. Нетрудно понять, что в переменной `a` меняются только младшие 7 битов. Эту переменную можно отождествлять с двоичным словом $a_6 \dots a_1 a_0$ (a_0 — самый младший бит) или с вектором $(a_0, a_1, \dots, a_6)$ над полем $\mathbb{F}_2$. Обработка запроса `"Ring ring ring"` состоит в умножении этого вектора на матрицу

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Обработка запроса `"In the flat field"` состоит в умножении вектора на матрицу $A+I$, где I — единичная матрица порядка 7.

Характеристический многочлен матрицы A равняется $f(x) = x^7 + x + 1$. Матрица является корнем своего характеристического многочлена и, следовательно, $A^7 = A + I$. Характеристический многочлен является примитивным и поэтому показатель $e = 127$ — это минимальное натуральное такое, что $A^e = I$. При этом

$$A^{127} = A^{7 \cdot 18} \cdot A = (A + I)^{18} A.$$

Поэтому для того, чтобы как можно быстрее вернуться к первоначальному вектору требуется 18 раз послать запрос `"In the flat field"` и один раз запрос `"Ring ring ring"`. Быстрее нельзя. □