11 Умножение многочленов

Задача. Боб реализует умножение многочленов над полем из двух элементов. Многочлены задаются двоичными словами по правилам СТБ 34.101.31. Боб утверждает, что при определенном заполнении массивов `log1`, `log2`, `crt1`, `crt2` следующая программа на языке C++ реализует умножение многочлена `a` на многочлен `b`:

```
uint16 mul8x8(uint8 a, uint8 b)
{
  static const uint8 log1[256] = {???};
  static const uint8 log2[256] = {???};
  static const uint16 crt1[256] = {???};
  static const uint16 crt2[256] = {???};

  if (a == 0 || b == 0)
    return 0;

  uint16 d1, d2;
  if (((d1 = log1[a]) += log1[b]) > 255)
    d1 -= 255;
  if (((d2 = log2[a]) += log2[b]) > 255)
    d2 -= 255;

  return crt2[d1] ^ crt1[d2];
}
```

Восстановите заполнение массивов.

Решение. Будем рассматривать многочлены над полем $\mathbb{F}_2$. Нам требуется перемножить многочлены $a(x)$, $b(x)$, степени которых меньше 8. Многочлены представляются октетами.

Выберем примитивный многочлен $f_1(x)$ степени 8. Если $a(x) \neq 0$, то $a(x) = x^d \bmod f_1(x)$ для некоторого $d \in \{0, 1, \ldots, 254\}$. Действительно, в противном случае $x^{d_1} \equiv x^{d_2} \pmod{f_1(x)}$ для некоторых $0 \leq d_1 < d_2 \leq 254$, т.е. $f_1(x) \mid x^{d_2-d_1} - 1$, что противоречит примитивности $f_1(x)$.

Величину d, которая фигурирует в представлении $a(x)$ назовем логарифмом по модулю $f_1(x)$ и обозначим через $\log a(x) \bmod f_1(x)$. Таблицу логарифмов сохраним в массиве `log1`.

Выберем еще один примитивный многочлен $f_2(x)$ степени 8, отличный от $f_1(x)$. Логарифмы по модулю $f_2(x)$ сохраним в массиве `log2`.

Пусть

$$d_1 = (\log a(x) \bmod f_1(x) + \log b(x) \bmod f_1(x)) \bmod 255,$$
$$d_2 = (\log a(x) \bmod f_2(x) + \log b(x) \bmod f_2(x)) \bmod 255.$$

Тогда

$$a(x)b(x) \equiv x^{d_i} \pmod{f_i(x)}, \quad i = 1, 2.$$

Мы имеем дело с китайской системой сравнений, которую можно решить методом Гаусса:

$$a(x)b(x) = \left(f_2^*(x)f_2(x)x^{d_1} + f_1^*(x)f_1(x)x^{d_2}\right) \bmod f_1(x)f_2(x).$$

Здесь $f_1^*(x) = f_1(x)^{-1} \bmod f_2(x)$, $f_2^*(x) = f_2(x)^{-1} \bmod f_1(x)$.

В программе решение системы реализовано обращениями к массивам, задающим отображения

$$d \mapsto f_i^*(x)f_i(x)x^d \bmod f_1(x)f_2(x).$$

При $f_1(x) = x^8 + x^4 + x^3 + x^2 + 1$ и $f_2(x) = x^8 + x^6 + x^5 + x^4 + 1$ (возвратный к f_1) получаем следующее заполнение массивов: `http://apmi.bsu.by/assets/files/tasks/task11.zip`.