12 Деление многочленов

Задача. Боб реализует деление многочленов над полем из двух элементов. Многочлены задаются двоичными словами по правилам СТБ 34.101.31. Боб написал программу на языке C++, в которой многочлен, заданный строкой октетов `poly`, нацело делится на многочлен $g(x)$.

```
void polyDiv(uint8* poly, size_t n)
{
  uint8 a = 0;
  for (int i = 0; i < n; i++)
  {
     a ^= poly[i];
     a ^= a << 2;
     a ^= a << 4;
     poly[i] = a;
     a >>= 6;
  }
}
```

Найдите $g(x)$.

Решение. Пусть $f(x) = a_{n-1}(x)x^{(n-1)w} + \ldots + a_1(x)x^w + a_0(x)$, где $\deg a_i < w$. Пусть $g(x)$ делит $f(x)$ и $\deg g < w$.

Предположим, что

$$f(x)/g(x) = b_{n-1}(x)x^{(n-1)w} + \ldots + b_1(x)x^w + b_0(x),$$

где $\deg b_i < w$. Тогда

$$a_{n-1}(x)x^{(n-1)w} + \ldots + a_1(x)x^w + a_0(x) = g(x)(b_{n-1}(x)x^{(n-1)w} + \ldots + b_1(x)x^w + b_0(x)).$$

При этом

$$a(x) \equiv g(x)b_0(x) \pmod{x^w}$$

и

$$b_0(x) = a(x)g^*(x) \bmod x^w,$$

где $g^*(x) = g(x)^{-1} \bmod x^w$.

После определения b_0 можно определить b_1, использовав соотношение

$$(f(x) - g(x)b_0(x))/x^w = g(x)(b_{n-1}(x)x^{(n-2)w} + \ldots + b_2(x)x^w + b_1(x)),$$

затем b_2 и так далее.

В программе $w = 8$, $g^*(x) = (x^2 + 1)(x^4 + 1) = (x + 1)^6$ и, следовательно,

$$g(x) = (x + 1)^2 = x^2 + 1.$$