33 2014

Задача. В СТБ 34.101.31 используется операция умножения в поле из 2^{128} элементов. Умножение обладает следующим свойством: возведение в квадрат $a * a$ выполняется значительно быстрее, чем общее умножение $a * b$. Поэтому при возведении элемента a в определенную степень важно организовать вычисления так, чтобы минимизировать число общих умножений, не обращая внимания на число возведений в квадрат. Можно ли найти a^{2014} с помощью 5 умножений? С помощью 4 умножений?

Решение. Пусть натуральное число d представляется двоичным словом $d_{l-1} \dots d_1 d_0$:

$$d = \sum_{i=0}^{l-1} d_i 2^i.$$

Пусть $w(d)$ — вес Хэмминга этого слова — число его единичных разрядов. Возведениями a^d в квадрат можно построить элементы $a^{2^s d}$, $s = 1, 2, \dots$. Соответствующие показатели $2^s d$ получены сдвигом двоичной записи d на s позиций вправо. Для этих показателей $w(2^s d) = w(d)$.

С помощью умножения a^d на a^e можно перейти к показателю $d + e$ с весом Хэмминга

$$w(e + d) \le w(e) + w(d). \qquad (\star)$$

Докажем это неравенство. Будем просматривать разряды e и d справа налево, от младших к старшим. Если пара разрядов отличается от $(1, 1)$, то

$$w(e_{l-1} \dots e_1 e_0 + d_{l-1} \dots d_1 d_0) = w(e_{l-1} \dots e_1 + d_{l-1} \dots d_1) + e_0 + d_0.$$

Пусть $(e_0, d_0) = \dots = (e_{r-1}, d_{r-1}) = (1, 1)$, а $(e_r, d_r) \ne (1, 1)$. Пусть, например, $e_r = 0$. Тогда

$$w(e_{l-1} \dots e_1 e_0 + d_{l-1} \dots d_1 d_0) = w(e_{l-1} \dots e_{r+1} 1 + d_{l-1} \dots d_{r+1} d_k).$$

Из полученных равенств по индукции получаем оценку $(\star)$.

Оценка означает, что для вычисления a^d требуется затратить не менее $\lceil \log_2 w(d) \rceil$ умножений. В частности, для $d = 2014 = 11111011110$ с весом $w(d) = 9$ требуется затратить не менее 4 умножений.

Четырех умножений достаточно:

$$\begin{aligned} a^3 &= a * a^2, \\ a^{15} &= a^3 * (a^3)^4, \\ a^{495} &= a^{15} * (a^{15})^{32}, \\ a^{2014} &= (a^{495} * a^{512})^2. \end{aligned}$$

□