Алгоритм быстрого возведения в степень

$y = a^x \bmod p$ – хотим вычислить

Введем $t = \lfloor \log_2 x \rfloor$

Вычисляем $a, a^2, a^4, a^8, \ldots, a^{2t} \bmod p$

И записываем x в двоичной системе

$x = (x_t\, x_{t-1} \ldots x_1\, x_0)_2$

Тогда $y = a^x \bmod p = \prod_{i=0}^{t} a^{x_i \cdot 2^i} \bmod p$

Пример: $3^{100} \bmod 7$

$t = \lfloor \log 100 \rfloor = 6$

$a = 3 \quad a^2 \bmod 7 = 2 \quad a^4 \bmod 7 = 4$

$a^8 \bmod 7 = 2 \quad a^{16} \bmod 7 = 4 \quad a^{32} \bmod 7 = 2$

$a^{64} \bmod 7 = 4$

$100 = 64 + 32 + 4 = (\overset{6}{1}\overset{5}{1}\overset{4}{0}\overset{3}{0}\overset{2}{1}\overset{1}{0}\overset{0}{0})_2$

$3^{100} \bmod 7 = a^{64} \cdot a^{32} \cdot a^4 = 4 \cdot 2 \cdot 4 = 32 \bmod 7$

$= 4$