Problem 5. «The shortest addition chain»

In many cryptographic systems we need to calculate the value $B = A^c \bmod p$, where A is an integer, $1 \leqslant A \leqslant p-1$, c is an arbitrary positive integer, and p is a large prime number. One possible way of reducing the computational load of calculating is to minimize the total number of multiplications required to compute the exponentiation. Since the exponent in equation is additive, the problem of computing powers of the base element A can also be formulated as an addition calculation, for which addition chains are used.

An **addition chain** for an integer n is a sequence of positive integers

$$a_0 = 1, a_1, \ldots, a_{r-1}, a_r = n,$$

where r is a positive integer (that is called the **length** of the addition chain) and the following relation holds for all i, $1 \leqslant i \leqslant r$:

$$a_i = a_j + a_k \text{ for some } k, j \text{ such that } k \leqslant j < i.$$

Find an addition chain of length as small as possible for the value 81, present it as a list of values and mathematically prove that it can not be shorter!

An example. For the value 15 the shortest additional chain has length 5 and its list of values is $1, 2, 3, 6, 12, 15$. So, to optimally calculate $B = A^{15} \bmod p$, one can use just five multiplications:

$$\begin{aligned} A^2 &= A \cdot A \mod p \\ A^3 &= A^2 \cdot A \mod p, \\ A^6 &= A^3 \cdot A^3 \mod p, \\ A^{12} &= A^6 \cdot A^6 \mod p, \\ A^{15} &= A^{12} \cdot A^3 \mod p. \end{aligned}$$