Let's consider the sequence of polynomials:

$$P_0(x) = x$$

$$P_n(x) = P_{n-1}^2(x) - 2$$

$$n \in \mathrm{N}$$

The polynomial degree is

$$k = 2^n$$

I noted that the coefficients of every polynomial could be easily factored. Namely, I conjecture that for n>0 the polynomial looks like

$$P_n(x) = \sum_{i=0}^{k/2} (-1)^{\frac{k}{2}-i} 2^{2n-2q_0(i)-q_1(i)-1} \beta_{2i}(k) x^{2i},$$

where $q_0(i)$ is the maximal power of 2 dividing i (i.e. the length of tip chain of zeros in binary representation of i) and $q_1(i)$ is the number of units in binary representation of i; $q_0(0)$ is equated to n–1. $\beta_{2i}(k)$ is odd and for every odd prime p the maximal power of p dividing $\beta_{2i}(k)$ equals to the number of positive integer m's satisfying inequality:

$$\left(\frac{k}{2} - i\right) \bmod p^m + (2i) \bmod p^m > p^m$$