Anwendung der Polynomdivision:

Algorithmus zum Aufdecken von Übertragungsfehlern durch Polynomdivision in $\mathbb{Z}/2\mathbb{Z}$

Sei $g \in \mathbb{Z}/2\mathbb{Z}[x]$ ein fest gewähltes Polynom vom Grad $\deg(g) = n$. Die zu übertragende Nachricht (das „Codewort“) sei $\big(a_m, a_{m-1}, \ldots, a_0\big)$ mit $a_i \in \big\{0, 1\big\}$, $i = 0, 1, \ldots, m$. Zu dem Codewort sei in $\mathbb{Z}/2\mathbb{Z}[x]$ das Polynom $f(x) := \sum_{i=0}^{m} a_i \cdot x^i$ definiert.

- **Schritt 1:**
  Teile $h(x) := f(x) \cdot x^n$ durch $g(x)$, wobei sich ein Rest $r(x)$ ergeben kann mit $\deg(r) < n$. Es gilt
  $$h(x) \;=\; g(x) \cdot q(x) + r(x) \;\;,\;\; q \in \mathbb{Z}/2\mathbb{Z}[x]$$

- **Schritt 2:**
  Übertrage das Codewort zu $\quad h(x) - r(x) = g(x) \cdot q(x), \quad$ das sich wegen $r(x) = -r(x)$ (es gilt $+1 = -1$ in $\mathbb{Z}/2\mathbb{Z}$!!) aus dem Codewort von f (also der ursprünglichen Nachricht) und weiteren n Prüfbits (dem Codewort von $-r(x)$) zusammensetzt:

Nachricht	n Prüfbits
$a_m a_{m-1} \ldots a_1 a_0$	$01101 \ldots 0$
$\widehat{=} f(x)$	$\widehat{=} -r(x)$
$\widehat{=} h(x) - r(x) = g(x) \cdot q(x)$	

- **Schritt 3:**
  Der Empfänger dividiert das der empfangenen Nachricht entsprechende Polynom $p(x)$, das bei korrekter Übertragung also gerade $g(x) \cdot q(x)$ ist, durch $g(x)$.
  - Falls dabei ein Rest bleibt, dann liegt definitiv ein Übertragungsfehler vor, der in einigen Fällen sogar bestimmt und korrigiert werden kann.
  - Sonst ist ein Übertragungsfehler „eher unwahrscheinlich“.