

Parameters: polynomials u, v

precondition: $v \neq "0"$

$\frac{u}{v} = q$ (quotient), r (remainder)

postcondition: $u = q * v + r$

Assume for any polynomial p : $p.\text{leadingTerm} = p[p.\text{degree}] * x^{p.\text{degree}}$

Pseudocode:

$q = 0$

$r = u$

while $r \neq "0"$ and $r.\text{degree} \geq v.\text{degree}$

$t = \frac{r_{old}.\text{leadingTerm}}{v.\text{leadingTerm}}$ (t = temporary, single-term poly)

$q_{new} = q_{old} + t$

$r_{new} = r_{old} - t * v$

invariant: $u = q * v + r$

Base case:

$u = q * v + r = 0 * v + u = 0 + u = u$ [TRUE]

Iteration k (assume true):

$u = q_{old} * v + r_{old}$

Iteration k + 1:

$$u = q_{new} * v + r_{new} \implies \frac{u}{v} = q_{new} + \frac{r_{new}}{v} = (q_{old} + t) + \frac{(r_{old} - t * v)}{v} = q_{old} + \frac{r_{old}}{v}$$
$$\frac{u}{v} = q_{old} + \frac{r_{old}}{v} \implies u = q_{old} * v + r_{old} \text{ [TRUE]}$$

Termination:

$D = r.\text{degree} - v.\text{degree} + 1$

\implies Loop exits when $r.\text{degree} < v.\text{degree}$ ($D_{\text{minimum}} = 0$, given degrees are integers)

\implies Initially: $D > 0$, when $r.\text{degree} \geq v.\text{degree}$

For $r.\text{degree}$ to decrease after every iteration, r_{old} 's leading term must be removed at every iteration.

Given: $r_{new} = r_{old} - t * v$. To ensure r_{old} 's leading term is removed after every iteration, the following cases must hold true:

A) degrees must cancel out $\implies r_{old}.\text{degree} = t.\text{degree} + v.\text{degree}$

$$t = \frac{r_{old}.\text{leadingTerm}}{v.\text{leadingTerm}} \implies t.\text{degree} = r_{old}.\text{degree} - v.\text{degree}$$

$$r_{old}.\text{degree} = (r_{old}.\text{degree} - v.\text{degree}) + v.\text{degree} = r_{old}.\text{degree} \text{ [TRUE]}$$

B) coefficients must cancel out $\implies r_{old}[r_{old}.\text{degree}] = t[t.\text{degree}] * v[v.\text{degree}]$

$$t = \frac{r_{old}.\text{leadingTerm}}{v.\text{leadingTerm}} \implies t[t.\text{degree}] = \frac{r_{old}[r_{old}.\text{degree}]}{v[v.\text{degree}]}$$

$$r_{old}[r_{old}.degree] = \left(\frac{r_{old}[r_{old}.degree]}{v[v.degree]} \right) * v[v.degree] = r_{old}[r_{old}.degree] [TRUE]$$

\Rightarrow r_{old} 's leading term is always removed \Rightarrow $r.degree$ decreases after every iteration, $v.degree$ does not change \Rightarrow D decreases after every iteration until $D \leq 0 \Rightarrow$ LOOP EXITS [TRUE]