CSC375F Reducing polynomial division to multiplication

Here is how we can reduce polynomial multiplication to addition so that if we can compute multiplication of nth degree polynomials within $M(n)$ arithmetic operations, then division of an n^{th} degree polynomial can be computed in $O(M(n))$ arithmetic operations.

Say we wish to divide $A(x) = \sum_{k=0}^{n} a_k x^k$ by $B(x) = \sum_{k=0}^{m} b_k x^k$; that is compute $Q(x)$ and $R(x)$ such that $A(x) = Q * B + R$ with degree $R <$ degree $B = m$. Without loss of generality we can assume $m \leq n$ and $b_m = 1$ and it suffices to compute $Q(x)$.

Substituting $x = 1/z$, we get:

$$\sum_{k=0}^{n} a_k z^{-k} = \sum_{k=0}^{n-m} q_k z^{-k} * \sum_{k=0}^{m} b_k z^{-k} + \sum_{k=0}^{m-1} r_k z^{-k}$$

Multiplying by z^n we obtain:

$$\sum_{k=0}^{n} a_{n-k} z^k = \sum_{k=0}^{n-m} q_{n-m-k} z^k * \sum_{k=0}^{m} b_{m-k} z^k + \sum_{k=0}^{m-1} r_{m-1-k} z^{n-m+1+k}$$

Taking this equation mod z^{n-m+1} we eliminate the $\{r_j\}$ coefficients to get:

$$\sum_{k=0}^{n-m} a_{n-k} z^k = \sum_{k=0}^{n-m} q_{n-m-k} z^k * \sum_{k=0}^{n-m} b_{m-k} z^k$$

Our problem has now been reduced to the problem of computing the power series inverse of $B'(z) = \sum_{k=0}^{n-m} b_{m-k} z^k$. But since we are only trying to compute the $\{q_j\}$ coefficients up to $j = n - m$, we need only compute the power series inverse mod z^{n-m+1}. To simplify notation, lets refer to B' as U and the power series inverse as V so that $U * V = 1$. Since $b_m = b'_0 = 1$ we are assuming the constant term u_0 of U is equal to 1 and hence $V mod z^1 = 1$.

We will compute V mod z^j for using Newton iteration. Let $f(y) = (\frac{1}{y} - U)$. We are then trying to compute a root of f in the power series ring. By the quadratic convergence of Newton iteration, we can show that if $(y - \beta) = 0$ mod z^j then $\phi(y) - \beta = 0$ mod z^{2j} where

$$\phi(y) = y - \frac{f(y}{f'(y)} = y - \frac{\frac{1}{y} - U}{-\frac{1}{Y^2}} = 2y - Uy^2$$

Thus, $\phi(y) - V = y - V + y - Uy^2$
$= y - V + y - y^2/V$ since $U * V = 1$
$= y - V - (\frac{y}{V})(y - V)$
$= (1 - \frac{y}{V})(y - V)$
$= \frac{1}{V}(V - y)(y - V)$
$= -U(y - V)^2$ again using $U * V = 1$.

Hence if we had a β such that $y - V = y - \beta = 0$ mod z^j then $\phi(y) - V = \phi(y) - \beta = 0$ mod z^{2j}'.

The resulting recursion is $D(2j) = D(j) + O(M(2j)$ with $D(1) = O(1)$ so that $D(n) - O(M(n))$.