Complexity of Classical Algorithms for $\mathbb{Z}$ and $F[x]$.

Michael Monagan

Let $a, b \in \mathbb{Z}$, B be a constant, $0 < a < B^n$, $0 < b < B^m$, $n \geq m$.
In the tables EEA = Extended Euclidean Algorithm.

$a \pm b$	$O(n)$
$a \times b$	$O(nm)$
$a \div b$	$O((n-m+1)m)$
$\gcd(a, b)$	$O(nm)$
$\text{EEA}(a, b)$	$O(nm)$

Table 1: Complexity for integer operations

Let f, g be non-zero polynomials in $F[x]$, F a field.
Let $n = \deg f$, $m = \deg g$, $n \geq m$, $\alpha \in F$.

$f \pm g$	$O(n)$
$f \times g$	$O(nm)$
$f \div g$	$O((n-m+1)m)$
$\gcd(f, g)$	$O(nm)$
$\text{EEA}(f, g)$	$O(nm)$
$f(\alpha)$	$O(n)$
interpolate f	$O(n^2)$

Table 2: Number of arithmetic operations in F for polynomials