Division with remainder
A more familiar setting: the integers $\mathbb{Z}$

For all $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{>0}$, there exist unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r \quad \text{and} \quad 0 \leq r < b$$

**Algorithms:** suppose $b$ has (exactly) $n$ bits and $a$ is at most $2^n$ bits

- grade school algorithm: time $O(n^2)$
- *general fact:* division is no harder than multiplication
Polynomial division with remainder

Let $f, g \in R[X]$ with $g$ monic (i.e., leading coefficient 1) There exist unique $q, r \in R[X]$ such that

$$f = gq + r \text{ and } \deg(r) < \deg(g)$$

Fact: if $\deg(f) \geq \deg(g)$, then $\deg(q) = \deg(f) - \deg(g)$

Algorithms:

- grade school: quadratic time
- general fact: division is no harder than multiplication

Note: if we compute $q$, we can compute $r$ as $r = f - gq$, using a single polynomial multiplication

$\implies$ Let’s focus on computing $q$
Preliminaries: the polynomial “reverse” operation

Suppose \( f = \sum_{i=0}^{m} a_i X^i \), with \( a_m \neq 0 \) (so \( \deg(f) = m \))

Define the reverse of \( f \): \( \text{Rev}(f) = \sum_{i=0}^{m} a_i X^{m-i} \)

Suppose \( g \in R[X] \), monic, \( \deg(g) = n \leq m \), and let

\[ f = gq + r \quad (\deg(r) < n, \ \deg(q) = m - n) \]

Lemma 1:

\[ \text{Rev}(f) \equiv \text{Rev}(g) \text{Rev}(q) \pmod{X^{m-n+1}} \]

Notation: \( u \equiv v \pmod{X^k} \) means \( u = v + X^k w \) for some polynomial \( w \)
Polynomial arithmetic mod $X^k$

$u \equiv v \pmod{X^k} \iff$ low-order $k$ terms of $u$ and $v$ agree

If $u \equiv u' \pmod{X^k}$ and $v \equiv v' \pmod{X^k}$, then

$u + v \equiv u' + v' \pmod{X^k}$ and $u \cdot v \equiv u' \cdot v' \pmod{X^k}$

**Lemma 2:** If $u \in R[X]$ with constant term 1 and $k$ is a positive integer, there exists $v \in R[X]$ such that $uv \equiv 1 \pmod{X^k}$

*Note:* $v$ is called an inverse of $u$ mod $X^k$
Using the lemmas

Since $g$ is monic, $\text{Rev}(g)$ has constant term 1

Lemma 2 says $\text{Rev}(g)$ has an inverse $\nu$ mod $X^{m-n+1}$:

$$\text{Rev}(g) \cdot \nu \equiv 1 \pmod{X^{m-n+1}}, \quad \deg(\nu) \leq m - n$$

Lemma 1 says

$$\text{Rev}(f) \equiv \text{Rev}(g) \text{Rev}(q) \pmod{X^{m-n+1}} \quad (\ast)$$

Multiply both sides of $(\ast)$ by $\nu$:

$$\nu \text{Rev}(f) \equiv \nu \text{Rev}(g) \text{Rev}(q) \equiv 1 \cdot \text{Rev}(q)$$

$$\equiv \text{Rev}(q) \pmod{X^{m-n+1}}$$

Overall strategy to compute $q$:

1. Compute inverse $\nu$ of $\text{Rev}(g)$ mod $X^{m-n+1}$
2. Compute the product $p = \nu \text{Rev}(f)$
3. Output the low-order $m - n + 1$ terms of $p$, reversed
Lemma 1:

\[ \text{Rev}(f) \equiv \text{Rev}(g) \text{Rev}(q) \pmod{X^{m-n+1}} \]

Proof:

Observation: if \( f = \sum_{i=0}^{m} a_i X^i \), then

\[
\text{Rev}(f) = \sum_{i=0}^{m} a_i X^{m-i} = X^m \sum_{i=0}^{m} a_i X^{-i} = X^m f(X^{-1})
\]

Since \( f = gq + r \), with \( \deg(r) < n \), we have

\[
\text{Rev}(f) = X^m f(X^{-1}) = X^m \left( g(X^{-1})q(X^{-1}) + r(X^{-1}) \right)
= X^n g(X^{-1}) \cdot X^{m-n} q(X^{-1}) + X^m r(X^{-1})
= \text{Rev}(g) \text{Rev}(q) + X^m r(X^{-1})
\equiv \text{Rev}(g) \text{Rev}(q) \pmod{X^{m-n+1}}
\]
Lemma 2: If \( u \in R[X] \) with constant term 1 and \( k \) is a positive integer, there exists \( v \in R[X] \) such that \( uv \equiv 1 \pmod{X^k} \)

Proof: We will give a proof by induction that naturally leads to an efficient “divide and conquer” algorithm.

Base case, \( k = 1 \): since \( u \equiv 1 \pmod{X} \), we can take \( v = 1 \).
Inductive step, \( k > 1 \):
Let \( k = \lfloor k/2 \rfloor \) and suppose \( uv_0 \equiv 1 \pmod{X^l} \)
This means \( uv_0 = 1 + X^l w \) for some \( w \in R[X] \)
We shall write
\[
u(\nu_0 + X^l \nu_1) \equiv 1 \pmod{X^k}
\]
and solve for \( \nu_1 \)
We have
\[
u(\nu_0 + X^l \nu_1) = uv_0 + X^l uv_1 = 1 + X^l (w + uv_1)
\]
So it suffices to find \( \nu_1 \) such that
\[
w + uv_1 \equiv 0 \pmod{X^{k-l}}
\]
and \( \nu_1 := -\nu_0 w \) does the job, since
\[
w + uv_1 \equiv w - uv_0 w = w(1 - uv_0) \equiv 0 \pmod{X^l}
\]
Algorithm $\text{Invert}(u, k)$:

Input: $u \in R[X]$ with constant term 1 and $\deg(u) < k$

Output: $v \in R[X]$ with $uv \equiv 1 \pmod{X^k}$ and $\deg(v) < k$

If $k = 1$, return 1

Otherwise, recursively compute

$$v_0 := \text{Invert}(u_0, \ell)$$

where $\ell := \lceil k/2 \rceil$ and $u_0 :=$ low-order $\ell$ terms of $u$

Compute $u \cdot v_0$, which is of the form $1 + X^\ell w$

Compute $v_1 := -v_0 \cdot w$

Set $v :=$ low-order $k$ terms of $v_0 + X^\ell v_1$

Return $v$
Running time analysis

Suppose we can multiply polynomials of degree at most \( k \) using \( M(k) \) operations in \( R \)

Let \( T(k) \) be the number of operations performed by the recursive inversion algorithm

We have

\[
T(k) \leq T(\lceil k/2 \rceil) + O(M(k))
\]

This implies \( T(k) = O(M(k)) \)

*Technical note*: this assumes \( M(k) \) is “reasonable”:

\[
1 \leq \frac{M(a + b)}{M(a) + M(b)} \leq C
\]

for some constant \( C \) and all \( a, b \)
Summary:

- Polynomial division is no harder than multiplication (up to a constant factor)
  
  - More formally: given \( f, g \in R[X] \), where \( g \) is monic, \( \deg(g) = n \), and \( \deg(f) < 2n \), we can compute \( q, r \in R[X] \) such that \( f = gq + r \) and \( \deg(r) < n \) using \( O(M(n)) \) operations in \( R \)

- The same holds for integer division (details are slightly messier)