1. Polynomials
2. Division Algorithm

$\mathbb{F}[x]$

$$f(x)=\sum_{j=0}^{n} a_j x^j \qquad a_j \in \mathbb{F}$$

Equality: $f(x)=\sum_{j=0}^{n} a_j x^j \qquad g(x)=\sum_{j=0}^{n} b_j x^j$

$f(x)=g(x)$ when $a_j=b_j$ for all $j\in\{0,\dots,n\}$

Addition: $f(x)+g(x)=\sum_{j=0}^{n}(a_j+b_j)x^j$

Multiplication: $f(x)=1+2x+3x^2+4x^3$

$g(x)=2-x-3x^2$

$f(x)g(x)$: Constant: $1\cdot 2=2$

x: $1\cdot(-x)+2x\cdot 2=(-1+4)x=3x$

x^2: $1\cdot 3x^2+2x(-x)+(-3)x^2\cdot 2=-5x^2$

$f(x)g(x)$ Coeff of x^m is $\sum_{k=0}^{m} a_k b_{m-k} = a_0 b_m + a_1 b_{m-1} + \dots + a_m b_0$

$$f(x)g(x)=\sum_{m>0}\left(\sum_{k=0}^{m} a_k b_{m-k}\right)x^m$$

$$\Updownarrow$$

$$\sum_{m=0}^{\deg(f(x)+g(x))}$$

Power Series: $f(x) = 1 + x + x^2 + \dots = \sum_{n=0} x^n = \frac{1}{1-x}$

$$f(x)^2 = 1 + 2x + 3x^2 + 4x^3 + \dots = \frac{1}{(1-x)^2}$$

$f(x)^3$ Coeff of x^n is $(n+1) + n + (n-1) + \dots + 1 = \frac{(n+1)(n+2)}{2}$

$$\frac{1}{(1-x)^3} = \sum_{n \geq 0} \binom{n+2}{2} x^n \qquad = \binom{n+2}{2}$$

Division Algorithm for polys

$\mathbb{C}[x]$ Divide $f(z) = (-1+2i)z^3 + 2z^2 + 3iz - 1$ by $g(z) = (1-2i)z + i$

Quotient: $-z^2 + iz + (-1+i)$ — $q(z)$

$$(1-2i)z + i \;\overline{\big)\, (-1+2i)z^3 + 2z^2 + 3iz - 1}$$

$$(-1+2i)z^3 - iz^2$$

$$\overline{\qquad (2+i)z^2 + 3iz}$$

$$(2+i)z^2 - z$$

$$\overline{\qquad (1+3i)z - 1}$$

$$(1+3i)z + (i-1)$$

$$\overline{\qquad -i}$$

$r(z)$

$(1-2i)z\,\square = (2+i)z^2$

$\square = \frac{(2+i)z}{(1-2i)}$

$\square = iz$

$\frac{3i+1}{1-2i} \cdot \left(\frac{1+2i}{1+2i}\right)$

$= -1+i$

$$f(z) = q(z)g(z) + r(z)$$

$$\deg(r(z)) < \deg(g(z)) \text{ or } r(z) = 0$$

Div. Algorithm for Poly: If $f(x), g(x) \in \mathbb{F}[x]$ and $g(x)$ is not the zero poly, then there exist unique $q(x), r(x) \in \mathbb{F}[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

where $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$

Proof: Excercise.

$\mathbb{Z}_3[x]$ $\quad f(x) = x^4 + [2]x^3 + x \quad g(x) = x^2 + [2]$

$$
\begin{array}{r|l}
 & x^2 + [2]x + [1] \\
\hline
x^2 + [2] & x^4 + [2]x^3 \qquad\qquad + x \\
 & x^4 \qquad + [2]x^2 \\
\hline
 & [2]x^3 + x^2 + x \\
 & [2]x^3 \qquad + x \\
\hline
 & x^2 \\
 & x^2 \qquad + [2] \\
\hline
 & [1]
\end{array}
$$

$q(x) = x^2 + [2]x + [1]$

$r(x) = [1]$

$\mathbb{Z}_4[x]$ ($\mathbb{Z}_4$ is not a field)

$$
\begin{array}{r|l}
 & ??? \\
\hline
[2]x & x
\end{array}
$$

not possible since [2] does not have an inverse.