What is $GF(p^k)$?

$$\boxed{\text{GF}(p^k) \text{ is the unique field of size } p^k \text{ (up to iso.)}}$$

How to see $GF(p^k)$?

Each ele of $GF(p^k)$ is a polynomial $f(x)$ of degree less than k with coeff. a_i in $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$ for $i = 0, \cdots, k-1$.

$$f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} \in \mathbb{Z}_p[x]$$

Let $h(x)$ be a monic irreducible polynomial of degree k. Define $*$ in $GF(p^k)$ as

$$f(x), g(x) \in GF(p^k)$$

$$f(x) * g(x) = f(x) \cdot g(x) \mod h(x)$$

For $f(x) \in GF^*(p^k)$ $(GF(p^k) \setminus \{0\})$

(multiplicative) inverse of $f(x)$ can be calculated by extended Euclidean algo.

Eg: Define

$$GF(2^3) = \{0, 1, x, x+1, x^2, x^2+x, x^2+1, x^2+x+1\}$$

$$h(x) = x^3 + x + 1$$

Table 4.7 Polynomial Arithmetic Modulo $(x^3 + x + 1)$

		000	001	010	011	100	101	110	111
	+	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
000	0	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + 1$	$x^2 + x + 1$
001	1	1	0	$x + 1$	x	$x^2 + 1$	x^2	$x^2 + x + 1$	$x^2 + x$
010	x	x	$x + 1$	0	1	$x^2 + x$	$x^2 + x + 1$	x^2	$x^2 + 1$
011	$x + 1$	$x + 1$	x	1	0	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x^2
100	x^2	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$	0	1	x	$x + 1$
101	$x^2 + 1$	$x^2 + 1$	x^2	$x^2 + x + 1$	$x^2 + x$	1	0	$x + 1$	x
110	$x^2 + x$	$x^2 + x$	$x^2 + x + 1$	x^2	$x^2 + 1$	x	$x + 1$	0	1
111	$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x^2	$x + 1$	x	1	0

(a) Addition

×		000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+1	x^2	$x+1$

(b) Multiplication

From the table $(x)^{-1} = x^2+1 \mod x^3+x+1$

why? $x \cdot (x^2+1) = x^3+x = 1 \mod x^3+x+1$

$(x^2+x+1)^{-1} = x^2 \mod x^3+x+1$

why? $(x^2+x+1)(x^2) = x^4+x^3+x^2 = 1 \mod x^3+x+1$

In general, how to find the multiplication inverse?

Use Extended Euclidean Algorithm!

Eg. Find $(x^2+x+1)^{-1}$ mod x^3+x+1

$\gcd[(x^2+x+1), (x^3+x+1)] = 1$

$$
\begin{array}{c|c|c|c}
 & x^2+x+1 & x^3+x+1 & \\
x+1 & x^2+x & x^3+1 & x+1 \\
\hline
 & 1 & x &
\end{array}
$$

$$
\begin{array}{r}
x+1 \\
x^2+x+1 \,\big)\, \overline{x^3+x+1} \\
x^3+x^2+x \\
\hline
x^2+1 \\
x^2+x+1 \\
\hline
x
\end{array}
$$

$$1 = (x^2+x+1) - (x)(x+1)$$
$$= (x^2+x+1) - [(x^3+x+1) - (x^2+x+1)\cdot(x+1)](x+1)$$
$$= (x^2+x+1)(x^2) + (x^3+x+1)(x+1)$$

$\therefore (x^2+x+1)(x^2) = 1 - (x^3+x+1)(x+1)$

$= 1 \mod (x^3+x+1)$

$\therefore (x^2+x+1)^{-1} = x^2$

The Advanced Encryption Standard (AES) uses arithmetic in the finite field GF(2^8), with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Consider the two polynomials $f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$. Then

$$
\begin{aligned}
f(x) + g(x) &= x^6 + x^4 + x^2 + x + 1 + x^7 + x + 1 \\
&= x^7 + x^6 + x^4 + x^2
\end{aligned}
$$

$$
\begin{aligned}
f(x) \times g(x) = {} & x^{13} + x^{11} + x^9 + x^8 + x^7 \\
& + x^7 + x^5 + x^3 + x^2 + x \\
& + x^6 + x^4 + x^2 + x + 1 \\
= {} & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1
\end{aligned}
$$

$$
\begin{array}{r|cccccccccc}
 & x^5 & +x^3 & & & & & & & & \\
\hline
x^8 + x^4 + x^3 + x + 1 & x^{13} & +x^{11} & +x^9 & +x^8 & +x^7 & +x^6 & +x^5 & +x^4 & +x^3 & +1 \\
 & x^{13} & & +x^9 & +x^8 & & +x^6 & +x^5 & & & \\
\cline{2-8}
 & & x^{11} & & & & & & +x^4 & +x^3 & \\
 & & x^{11} & & & +x^7 & +x^6 & & +x^4 & +x^3 & \\
\cline{3-10}
 & & & & & x^7 & +x^6 & & & & +1
\end{array}
$$

Therefore, $f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$.

Consider the two polynomials in GF(2^8) from our earlier example:

$$f(x) = x^6 + x^4 + x^2 + x + 1 \text{ and } g(x) = x^7 + x + 1.$$

$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1)$	$=$	$x^7 + x^6 + x^4 + x^2$	(polynomial notation)
$(01010111) \oplus (10000011)$	$=$	(11010100)	(binary notation)
$\{57\} \oplus \{83\}$	$=$	$\{D4\}$	(hexadecimal notation)[10]

In an earlier example, we showed that for $f(x) = x^6 + x^4 + x^2 + x + 1$, $g(x) = x^7 + x + 1$, and $m(x) = x^8 + x^4 + x^3 + x + 1$, we have $f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$.