F - a set
with two operations
$+$
$\cdot$

$\mathbb{F}_p = (\underbrace{\{0,1,2,\dots,p-1\}}, +_p, \cdot_p)$ | $(\mathbb{R}, +, \cdot)$

$\underline{+}$: $(F,+)$ - is a group (abelian)

$\exists e \in F \quad \forall a \in F \quad e+a = a+e = a$

$\forall a \in F \quad \exists a' \in F \quad a+a' = a'+a = e$

$\forall a,b,c \in F \quad (a+b)+c = a+(b+c)$

abelian group: $\forall a,b \in F \quad a+b = b+a$

$(\mathbb{R},+)$
$e=0$
$a \in \mathbb{R}$, $a' = -a$
$-a+a=0$, $a+(-a)=0$

$\cdot$: $(F\setminus\{0\}, \cdot)$ - is an abelian group

$+: F\times F \to F$, $\quad \cdot: F\setminus\{0\} \times F\setminus\{0\} \to F\setminus\{0\}$
$\cdot: F\times F \to F$

$(\mathbb{R}\setminus\{0\}, \cdot)$
$e=1$ $\quad \}\ e = I$
$a \in \mathbb{R}$, $a' = \frac{1}{a} = a^{-1}$
$a \cdot a^{-1} = 1$

$\mathbb{F}_p$: 0 - neutral element of addition

$a \in \{0,1,\dots,p-1\}$

$a+0 \pmod p \equiv a \pmod p$
$0+a \pmod p \equiv a \pmod p$

$a \neq 0$: $a+(p-a) \equiv p \pmod p \equiv 0 \pmod p$
$a=0$: $0+0 \pmod p$

$\boxed{\begin{aligned} &7+9 \pmod{11} \equiv \\ &\equiv 16 \pmod{11} \equiv \\ &\equiv 5 \pmod{11}\end{aligned}}$

$(\mathbb{F}_p \setminus \{0\}, \overset{\circ}{p})$

$1 \in \mathbb{F}_p \setminus \{0\} = \{1, 2, \dots, p-1\}$

$1 \cdot a \equiv a \pmod p$

$a \cdot 1 \equiv a \pmod p$

a^{-1}: - extended Euclidean algorithm:

$\gcd(a, b) = d$

$d = u \cdot a + v \cdot b \qquad u, v \in \mathbb{Z}$

$p = p$ - prime number

$a \in \{1, 2, \dots, p-1\}$

$\gcd(a, p) = 1$

$\underline{1 = u \cdot a + v \cdot p} \qquad u, v \in \mathbb{Z}$

$1 \equiv u \cdot a + v \cdot p \pmod p \equiv u \cdot a \pmod p \equiv (u \bmod p) \cdot \underbrace{(a \bmod p)}_{= a} \pmod p$

$u > 0 \qquad a^{-1} \equiv u \pmod p$

$u < 0 \qquad a^{-1} \equiv (p - u) \pmod p$

$\forall a, b \in \mathbb{F}_p \setminus \{0\} \; a \cdot b \equiv b \cdot a \pmod p$

$\forall a, b, c \in \mathbb{F}_p \setminus \{0\} \; (a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod p$

$\mathbb{F}_p[X]$

$f = X^n + a_{n-1} X^{n-1} + \dots + \cancel{a_0} + a_0$

f - irreducible in $\mathbb{F}_p[X]$

- monic: $a_n = 1$

$\mathbb{F}_p[X] / (f)$

p^n