RECALL:

DEF A field is a set $\mathbb{F}$ equipped w/ two binary operations, $+$ and $\cdot$, satisfying, for all $a, b, c \in \mathbb{F}$:

(F1) (COMMUTATIVITY) $a + b = b + a$, $ab = ba$

(F2) (ASSOCIATIVITY) $a + (b + c) = (a + b) + c$,
$a(bc) = (ab)c$

(F3) (IDENTITY) There exist distinct elements $0, 1 \in \mathbb{F}$ such that $a + 0 = a$,
$a \cdot 1 = a$.

(F4) (INVERSES) For each $a \in \mathbb{F}$, there is $c \in \mathbb{F}$ such that $a + c = 0$.
For each nonzero $b \in \mathbb{F}$, there is $d \in \mathbb{F}$ such that $bd = 1$.

(F5) (DISTRIBUTIVE) $a(b + c) = ab + ac$

EX $\mathbb{R}$, $\mathbb{Q}$: fields
$\mathbb{Z}$: not field

EX $\mathbb{Z}_n$, integers modulo n w/ operations $+, \cdot$ $(n \geq 2)$

ALWAYS TRUE: (F1), (F2), (F3), (F5) definitely hold (CHECK!)

(F4): additive inverses ✓

(F4): multiplicative inverses??

$n = 2$ $\quad \mathbb{Z}_2 = \{0, 1\}$

Mult table:

	0	1
0	0	0
1	0	1

✓

$\mathbb{Z}_2$ is a **field**

$n = 3$ $\quad \mathbb{Z}_3 = \{0, 1, 2\}$

Mult table:

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

✓

$\mathbb{Z}_3$ is a **field**

$n = 4$ $\quad \mathbb{Z}_4 = \{0, 1, 2, 3\}$

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

2 has no multiplicative inverse modulo 4

$\mathbb{Z}_4$: not a field

ANSWER: $\mathbb{Z}_n$ is a field iff n is prime

First, suppose n is not prime.

Then there exist integers a, b such that

$1 < a \leq b < n$ and $ab = n$.

CLAIM a has no inverse modulo n

Suppose a has an inverse.

Then there exists $x \in \mathbb{Z}_n$ such that

$$ax = 1$$

$\Rightarrow$ in $\mathbb{Z}$, $ax \equiv 1 \pmod{n}$

$\Rightarrow \quad n \mid (ax-1)$

$\Rightarrow \quad ax - 1 = nj, \quad j \in \mathbb{Z}$

$\Rightarrow \quad ax - nj = 1$

$ax - abj = 1$

$a(x - bj) = 1$

$\Rightarrow \quad a \mid 1$

"a divides 1"

$\Rightarrow \Leftarrow$ (CONTRADICTION)

Ex $\mathbb{Z}_6$:

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

SO: $\mathbb{Z}_n$ is never a field when n is composite

Now, suppose p is a prime number.

By definition, the only positive divisors of p are $1, p$.

Suppose $x \in \mathbb{Z}_p$, $x \neq 0$

(That is, $x \not\equiv 0 \pmod{p}$ in $\mathbb{Z}$, so $p \nmid (x-0)$, i.e., $p \nmid x$)

Since $p \nmid x$, $\gcd(x, p) = 1$.

THM (GCD as linear combination)

Let $a, b \in \mathbb{Z}$, a, b not both 0.

There exist integers x, y such that

$$ax + by = \gcd(a, b),$$

and $\gcd(a, b)$ is the smallest such positive integer that can be written as a "linear combination" of a, b.

so: there exist integers s, t such that

$$xs + pt = 1$$

$$\Rightarrow \quad xs \equiv 1 \pmod{p}$$

so: take the class of s modulo p;

that is x^{-1}

EX $n = 7$, $x = 3$

There exist integers s, t such that

$$3s + 7t = 1$$

Actually: $3 \cdot 5 + 7 \cdot (-2) = 1$

$$3 \cdot 5 \equiv 1 \pmod 7$$

In $\mathbb{Z}_7$, $3^{-1} = 5$

NOTATION set S on which $+, \cdot$ are defined

$$S[t] := \left\{ \sum_{j=0}^{n} s_j t^j : n \in \mathbb{N} \cup \{0\}, s_j \in S \right\}$$

EX $\mathbb{Z}[x]$: polynomials w/ integer coefficients

For instance, $3x^2 - 2x + 42 \in \mathbb{Z}[x]$,

$-21 \in \mathbb{Z}[x]$,

etc.

Ex $\mathbb{Q}[\sqrt{3}] = \{ a + b\sqrt{3} : a, b \in \mathbb{Q} \}$

Is $\mathbb{Q}[\sqrt{3}]$ a field?

Comm (F1)? ✓ ($\mathbb{Q}[\sqrt{3}] \subseteq \mathbb{R}$)

Assoc (F2)? ✓ ($\mathbb{Q}[\sqrt{3}] \subseteq \mathbb{R}$) it inherits these properties from $\mathbb{R}$

Identities? (F3) $0 \in \mathbb{Q}[\sqrt{3}]$ additive id, $1 \in \mathbb{Q}[\sqrt{3}]$ mult. id. ✓

Dist (F5)? Subset of $\mathbb{R}$, so yes ✓

REALLY: Check closure under $+, \cdot$:

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a+c) + (b+d)\sqrt{3}$$ ✓

$$(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (bc + ad)\sqrt{3}$$ ✓

Inverses? (F4): If $a + b\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$,

then $(-a) + (-b)\sqrt{3}$ is its additive inverse.

Multiplicative inverses?

Suppose $a + b\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$.

$a + b\sqrt{3} \neq 0$

If $a = 0$, then $b\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$

$b \in \mathbb{Q}$, and, since $a = 0$, $b \neq 0$.

$\mathbb{Q}$: field, so there exists $b^{-1} \in \mathbb{Q}$ such that $bb^{-1} = 1$.

$(b^{-1})(b\sqrt{3}) = \sqrt{3}$

$(b^{-1}\sqrt{3})(b\sqrt{3}) = 3$

$\left(\frac{b^{-1}}{3}\sqrt{3}\right)(b\sqrt{3}) = 1$ ✓

If $b = 0$, then $a \neq 0$, $a \in \mathbb{Q}$, and a has inverse $a^{-1} \in \mathbb{Q}$. ✓

So: assume <u>both</u> $a, b \neq 0$.

<u>Ex</u> $1+\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$

$$(1+\sqrt{3})(1-\sqrt{3}) = \underset{(1)^2-(\sqrt{3})^2}{1-3} = 2$$

$$(1+\sqrt{3})\left(\tfrac{1}{2}-\tfrac{1}{2}\sqrt{3}\right) = 1 \quad \checkmark$$

Take $a+b\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$

$$(a+b\sqrt{3})(a-b\sqrt{3}) = a^2-3b^2$$

If $a^2-3b^2 \neq 0$, since it's a rational number, it has a mult. inverse: $\frac{1}{a^2-3b^2}$

so: $$(a+b\sqrt{3})\left(\frac{a}{a^2-3b^2}-\frac{b}{a^2-3b^2}\sqrt{3}\right) = 1$$ ✓

<u>Q</u>: Can $a^2-3b^2 = 0$???

$a, b \in \mathbb{Q}$, $a, b \neq 0$

Suppose $a^2 - 3b^2 = 0$

Then $a^2 = 3b^2$

$\Rightarrow a^2 (b^{-1})^2 = 3$

$\Rightarrow (ab^{-1})^2 = 3$

This implies that $\sqrt{3} = \pm ab^{-1}$

$\Rightarrow \sqrt{3} \in \mathbb{Q}$

$\Rightarrow\Leftarrow$, since $\sqrt{3}$ is irrational

Therefore, $\mathbb{Q}[\sqrt{3}]$ is a field.

Ex $\mathbb{Z}_2[\xi] = \{ a + b\xi : a, b \in \mathbb{Z}_2, \xi^2 + \xi + 1 = 0 \}$

Since $\xi^2 + \xi + 1 = 0$,

$\xi^2 = -\xi - 1 = \xi + 1$

(in $\mathbb{Z}_2$)

$\mathbb{Z}_2[\xi] = \{ 0, 1, \xi, \xi + 1 \}$

	0	1	ξ	$\xi+1$
0	0	0	0	0
1	0	1	ξ	$\xi+1$
ξ	0	ξ	$\xi+1$	1
$\xi+1$	0	$\xi+1$	1	ξ

$$\xi(\xi+1) = \xi^2 + \xi$$

$$\xi^2 + \xi + 1 = 0, \quad \text{so} \quad \xi^2 + \xi = 1$$

$\mathbb{Z}_2[\xi]$ is a field w/ four elements