We want to show that any finite field $F$ has $p^n$ elements where $p$ is a prime and $n$ a positive integer. Later on we will also construct such fields for different $p$ and $n$. So far we have only seen $F = \mathbb{Z}_p$, that is the case $n = 1$.

To prove that $|F| = p^n$ we need the concept of vector space:

**Def:** A vector space $V$ over a field $F$ is a set with two operations $+: V \times V \rightarrow V$ and $\cdot: F \times V \rightarrow V$ satisfying:

1. $u + (v + w) = (u + v) + w$
2. $u + v = v + u$
3. $\alpha(\beta u) = (\alpha \beta) u$
4. $1 \cdot u = u$
5. $0 \cdot u = 0$
6. $\alpha(u + v) = \alpha u + \alpha v$
7. $(\alpha + \beta)v = \alpha v + \beta v$

Here $u, v, w \in V$ and $\alpha, \beta \in F$.

Note that the multiplication is only defined for (element of field) \cdot (elt of vector space).

For $V = \mathbb{F}_p(\alpha_1, \alpha_2, \alpha_3)$ where $\alpha_i \in \mathbb{Z}_7$, it is a vector space over $\mathbb{Z}_7$ with $(\alpha_1, \alpha_2, \alpha_3) + (\beta_1, \beta_2, \beta_3) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \alpha_3 + \beta_3)$ and $\alpha(\alpha_1, \alpha_2, \alpha_3) = (\alpha \alpha_1, \alpha \alpha_2, \alpha \alpha_3)$.
In this example \( |V| = 7^3 \). But this is not a field we must know how to define mult. First.

\[ \text{Ex} \quad \text{The case } F = \mathbb{R} \text{ is well known from linear algebra, } \]
\[ \quad \text{and } V = \mathbb{R}^3 = \{ (x_1, x_2, x_3) \mid x_i \in \mathbb{R} \} \]

A number of concepts from vector spaces over \( \mathbb{R} \) can be defined in exactly the same way if \( \mathbb{R} \) is replaced by any field:

* \( u_1, u_2, \ldots, u_k \in V \) are called linearly dependent if there are \( x_1, \ldots, x_k \in F \), not all zero, such that \( x_1 u_1 + x_2 u_2 + \cdots + x_k u_k = 0 \).
* Linearly independent = not linearly dependent
* Basis = linearly independent and generates \( V \)
* Dimension = number of basis elements (can show that all bases have the same number of elements)

Ex. For a field and

\[ \text{Let } K \text{ be a subfield of } F. \text{ (That is } K \subseteq F \text{ and } K \text{ is itself a field.) Then } F \text{ is a vector space over } K. \]

Check the axioms. Now \( u_1, w \in F, \alpha, \beta \in K \subseteq F \)

They all follow from the fact that \( F \) is a field.
Since $F$ is finite, $F$ must have a finite basis $e_1, e_2, \ldots, e_n \in F$ as vector space over $K$. Now $F = \{x_1e_1 + \ldots + x_ne_n | x_i \in K \}$. 

$\Rightarrow |F| = |K|^n$.

If we could always find a subfield of $F$ of prime order this would prove that $|F| = p^n$ for some prime $p$.

We can find such a $K$: whenever $F$ is finite, let $K = \{1, 1+1, 1+1+1, 1+1+1+1, \ldots \} = \{1, 2, 3, 4, 5, \ldots \}$.

$F$ finite $\Rightarrow$ there are $r < s$ with $r \cdot 1 = s \cdot 1$ $\Rightarrow$ $(s-r) \cdot 1 = 0$ so there is some positive integer $m$ with $m \cdot 1 = 0$. The smallest such $m$ must be prime because if $m = a \cdot b$ with $1 < a, b < m$ then

$m \cdot 1 = (a \cdot 1) \cdot (b \cdot 1)$ and $F$ has no zero divisors.

so either $a \cdot 1 = 0$ or $b \cdot 1 = 0$ contradicting the minimality of $m$.

We conclude that $|F| = p^n$ for some prime $p$. $p$ is called the characteristic of the field $F$.
Polynomial rings

Ex If we want to construct a field with $7^3$ elements we start from $\mathbb{Z}_7[x]$ - polynomials with coefficients in $\mathbb{Z}_7$. Then we say that two polynomials $f, g$ are equivalent if they have the same remainder after division by $h(x) = x^3 + 2$.

We get equivalence classes of polynomials each having a representative $ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}_7$ and they can be added and multiplied:

$$(ax^2 + bx + c)(dx^2 + ex + f) =$$

$$adx^4 + (ae + bd)x^3 + (af + be + cd)x^2 + (bf + ce)x + cf$$

$$= ad(x(x^3 + 2) - 2x) + (ae + bd)((x^3 + 2) - 2) + (af + be + cd)x^2 + (bf + ce)x + cf \equiv ad(-2x) + (ae + bd)(-2) + (af + be + cd)x^2 + (bf + ce)x + cf.$$

Let us now formalise what we did above and see that we really get a field (if we choose $h(x)$ is a good way).
A polynomial with coefficients in a field \( F \) is an expression
\[
f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0
\]
We say that \( f = g \) if all coefficients agree.

\[\text{Example: let } f(x) = x^5 + x^2 - 3 \quad g(x) = x^2 + x + 2 \text{ over } \mathbb{Z}_5\]
One can check that \( f(0) = g(0) = 2 \quad f(1) = g(1) = 4 \)
\( f(2) = g(2) = 3 \quad f(3) = g(3) = 4 \quad f(4) = g(4) = 2 \) but even if all values at points of \( f \) and \( g \) are equal, \( f \) and \( g \) are different polynomials.

Now \( F[x] = \{\text{polynomials over } F\} \) is a ring and just as in \( \mathbb{R}[x] \) we can prove that the division algorithm, factor theorem and Euclidean algorithm for finding GCD all work.

\[\text{Example: find the greatest common divisor of } f(x) = x^3 + 2 \text{ and } g(x) = x^2 + 2 \text{ in } \mathbb{Z}_3[x]\]

Use the Euclidean algorithm
\[
\begin{align*}
x^3 + 2 & \overset{x}{\overline{-}} x^2 + 2 \\
\underline{x^3 + 2} & \\
- x^3 - 2x & \\
\underline{-2x + 2}
\end{align*}
\]

\[x^3 + 2 = (x^2 + 2)x + (-2x + 2)\]
\[
\begin{align*}
\frac{x+1}{x^2+2} &= \frac{-2x+2}{x^2+2} - \frac{x^2-2x}{x^2+2} \\
&= \frac{-2x+2}{x^2+2} - \frac{x+2}{x-2} \\
&= \frac{-2x+2}{x^2+2} - \frac{x-2}{x-2} \\
&= \frac{x+2}{x-2}\ 
\end{align*}
\]

Last non-vanishing remainder is \(-2x+2 = x+2\)

Hence \((f, g) = x+2\)

Let us now fix a polynomial \(h(x) \in F[x]\). As when we formed \(\mathbb{Z}_n\) we can say that two polynomials \(f, g \in F[x]\) are equivalent modulo \(h(x)\) if they have the same remainder after division by \(h(x)\). We can also show that addition and multiplication of congruency classes

\[[f(x)] + [g(x)] = [f(x)+g(x)] \] is well defined

\[[f(x)] \cdot [g(x)] = [(x) \cdot g(x)]\]

Just copy the proof from the construction of \(\mathbb{Z}_n\).

This results in the ring \(F[x]/(h(x))\) of congruency classes.
\( F[x]/(h(x)) \) is a field \( \iff \) \( h(x) \) cannot be factorised in \( F[x] \).

Such a polynomial is called an **irreducible** polynomial.

\[ h(x) = x^3 + 2 \text{ is irreducible in } \mathbb{Z}_7[x]: \]

If \( h \) was a product of factors of lower degree at least one of them would have degree one \( h(x) = h_1(x)h_2(x) \) \( h_1(x) = x - a \)

but then \( h(a) = 0 \) by the **factor theorem**

Does \( h(x) \) have a zero?

\[ h(0) = 2 \quad h(1) = 3 \quad h(2) = 10 = 3 \quad h(3) = 29 = 1 \]

\[ h(4) = h(-3) = -25 = 3 \quad h(5) = h(-2) = -6 = 1 \quad h(6) = h(-1) = 1 \]

No no zeroes so \( h \) cannot be reducible

This implies that \( \mathbb{Z}_7[x]/((x^3+2)) \) is a field

\& Find the inverse of \( x + 1 \) in \( \mathbb{Z}_7[x]/(x^3+2) \)

Divide \( x^3 + 2 \) by \( x + 1 \)

\[
\begin{array}{c}
\frac{x^2 - x + 1}{x + 1} \\
\frac{-x^2 + 2}{x + 2} \\
\end{array}
\]

\[
\begin{array}{c}
x + 2 \\
-(x + 1) \\
\end{array}
\]

\[
\Rightarrow \frac{x^3 + 2}{(x^2 - x + 1)(x + 1)} = x + 1
\]

Check: \( [x + 1][- x^2 + x + 1] = - x^3 + x^2 + x + 1 = - x^3 - 7 \)

\( = - x^3 + x^2 + x + 1 = [1] \)
Ex. 1.4.7 Factorize the following polynomials into irreducibles in \( \mathbb{Z}_3[x] \)

1. \( x^5 + x^4 + x^3 + x - 1 = f(x) \)
2. \( x^4 + 2x^2 + 2x + 2 = g(x) \)
3. \( x^4 + 1 = h(x) \)
4. \( x^8 + 2 = k(x) \)

1. First we search linear factors and by the factor theorem they correspond to zeros of the polynomial \( f(x) \)

\[ f(0) = -1 \quad f(1) = 3 = 0 \quad f(-1) = 0 \]

\( x = 1 \) is a zero \( \Rightarrow \) \( x - 1 \) is a factor \( \Rightarrow (x+1)(x-1) = x^2 - 1 \) is a factor

Divide:

\[ x^5 + x^4 + x^3 + x - 1 = (x^2 - 1)(x^3 + x^2 + 2x + 1) \]

Now if \( x^3 + x^2 + 2x + 1 \) was reducible it would have a linear factor and hence a zero, but it doesn’t have a zero. \( x^3 + x^2 + 2x + 1 \) must then be irreducible

Ans. \[ x^5 + x^4 + x^3 + x - 1 = (x-1)(x+1)(x^3 + x^2 + 2x + 1) \]

is a prime factorization
(2) Does \( g(x) = x^4 + 2x^2 + 2x + 2 \) have zeroes?

\[ \text{Ans: } x = -1 \text{ zero } \Rightarrow x+1 \text{ factor} \]

Divide:

\[ x^4 + 2x^2 + 2x + 2 = (x+1)(x^3 - x^2 + 2) \]

\( x^3 - x^2 + 2 \) has a zero \( x = -1 \) so we can divide by \( x+1 \) again

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

\( \text{zeros? } \emptyset, x \neq 1 \)

\( x^2 - 2x + 2 \) is of degree two with no zeroes and hence irreducible.

\[ \text{Ans: } x^4 + 2x^2 + 2x + 2 = (x+1)^2(x^2 - 2x + 2) \text{ is a prime factorisation.} \]

(3) \( h(x) = x^4 + 1 \) Zero? \( \&/1, x = \pm 1 \) No. If it is reducible it must be the product of two factors of degree 2:

\[ x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + x^3[a + c] + x^2[b + d + ac] + x[ad + bc] + bd \]

\[ \iff \begin{cases} a + c = 0 \\ b + d + ac = 0 \\ ad + bc = 0 \\ bd = 1 \end{cases} \]

\[ \text{Case I: } b = d = 1. \text{ \( x \) becomes:} \]

\[ \begin{cases} a + c = 0 \\ ac + 2 = 0 \iff \begin{cases} a = -c \\ -c^2 + 2 = 0 \text{ No sol!} \end{cases} \end{cases} \]

\( \text{Try } c = 0, 1, -1 \)
Case II  \( b = d = -1 \)  \((*)\) becomes

\[
\begin{cases}
  a = -c \\
  -c^2 - 2 = 0
\end{cases}
\] \(\iff\)

\[
\begin{cases}
  c = 1 \& a = -1 \\
  \text{or} \\
  c = -1 \& a = 1
\end{cases}
\]

\[
(x^2 - x - 1)(x^2 + x - 1)
\]

We know \( h(x) \) has no linear factors so

Ans  \( h(x) = (x^2 - x - 1)(x^2 + x - 1) \) is a prime factorisation

(4) \( k(x) = x^8 + 2 = x^8 - 1 = (x^4 - 1)(x^4 + 1) = (x^2 - 1)(x^2 + 1)(x^4 + 1) \)

\[
= (x-1)(x+1)(x^2+1)(x^4+1)
\]

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

\(\uparrow\)

No zeroes so tried [know factor from (3)]

Ans  \( k(x) = (x-1)(x+1)(x^2+1)(x^2-x-1)(x^2+x-1) \)