Fact: if \( \gcd(a, m) = 1 \), \( a \) has a multiplicative inverse \( \mod m \)

\[ \text{relatively prime} \]

\[ \exists x : xa \equiv 1 \pmod{m} \]

Equivalently, in \( \mathbb{Z}_m \)

\[ \exists b \in \mathbb{Z}_m : ba = 1 \]

\[ \text{multiplication in } \mathbb{Z}_m \]

[Why are these 2 statements equivalent?]

proof: We know that \( \exists u, v \in \mathbb{Z} : \)

\[ \gcd(a, m) = ua + mv = 1 \]

Since \( m \mid mv \) we have

\[ 1 \equiv u a \pmod{m} \]

which means that in \( \mathbb{Z}_m \)

\[ 1 = \hat{a} \cdot a \]

where \( \hat{a} = (u \mod m) \) [Why?]

But then \( \hat{a} \) is the required inverse. \( \square \)

We show, by example, how we can obtain the \( u, v \) in the eqn above, by extending Euclid's algorithm

Compute \( \gcd(162, 51) \)

\[ 162 = 3 \cdot 51 + 9 \quad (*) \]

\[ 51 = 5 \cdot 9 + 6 \quad (***) \]

\[ 9 = 1 \cdot 6 + 3 \quad (***) \]

\[ 6 = 2 \cdot 3 + 0 \]

(\( \text{so } \gcd(162, 51) = 3 \))

From (***), \( \gcd(162, 51) = 3 = 9 - 1 \cdot 6 \) [this would be the required equality for \( \gcd(3, 6) \) with \( u = 1, v = -1 \)]

substitute \( 6 \) from (**) \( \)

\[ 6 = 51 - 5 \cdot 9 \]

\[ \gcd(162, 51) = 3 = 9 - 1 \cdot [51 - 5 \cdot 9] = 9 - 51 + 5 \cdot 9 = -51 + 6 \cdot 9 \]

Substitute \( 9 \) from (*) \( \)

\[ 9 = 162 - 3 \cdot 51 \]

\[ \gcd(162, 51) = 3 = -51 + 6 \cdot [162 - 3 \cdot 51] = 6 \cdot 162 - 413 \cdot 51 \]

which gives \( u = 6 \) \( v = -15 \)
Some properties of $\mathbb{Z}_m$ +, * addition, multiplication in $\mathbb{Z}_m$

(i) $\forall a \in \mathbb{Z}_m \quad 0 + a = a + 0 = a$, $\forall a \in \mathbb{Z}_m \quad a \cdot 1 = a$

(ii) $\forall a \in \mathbb{Z}_m \quad \exists b \in \mathbb{Z}_m \quad a + b = 0 \quad b = -a$ 'additive inverse'
   For example, in $\mathbb{Z}_4$ the additive inverse of 2 is 2.

(iii) +, * are commutative, associative, and the distributive properties of +, * in $\mathbb{Z}$ hold.

(iv) if $a, m$ relatively prime $\left[\gcd(a, m) = 1\right]$ a has a multiplicative inverse.
   In particular, if $m$ is prime, every nonzero $a \in \mathbb{Z}_m$ has a multiplicative inverse.

This means that we know how to solve linear equations in $\mathbb{Z}_p$, $p$ prime:
   Find $x : a \cdot x + b = c$ (operations in $\mathbb{Z}_p$)
   
   $a \cdot x = c - b$ (add $-b$ to both sides -- it exists by (ii))
   $a^{-1} \cdot a \cdot x = a^{-1} (c - b)$ ( $a^{-1}$ exists by (iv))
   $x = a^{-1} (c - b)$

This also means we can solve congruences
   
   $a \cdot x + b \equiv c \pmod{p}$ $\alpha, \beta, y \in \mathbb{Z}$
   $x \equiv y - \beta \pmod{p}$

   [Of course, $a^{-1} = \left[a^{-1}\right]_m$]

Some more properties of divisibility, |, and of $\mathbb{Z}_m$

$\gcd(a, b) = 1 \land a \mid bc \rightarrow a \mid c$

Proof: $\exists x, y \in \mathbb{Z} \quad a \cdot x + b \cdot y = 1$ [Why?]
   multiply both sides by $c$
   $c \cdot a \cdot x + c \cdot b \cdot y = c$
   $a \mid c$ (because $a \mid b$)
   $a \mid (c + a \cdot b)$
   $a \mid c$

Thm If $a$ has a multiplicative inverse in $\mathbb{Z}_m$, it is unique.
   Proof: suppose by contradiction $\exists b, c : a \cdot b = a \cdot c = 1$. But we have

$$\begin{cases} b = b \cdot 1 \quad \text{(prop. of 1)} \\ b = b \cdot (a \cdot c) \quad \text{(hypothesis)} \\ b = (b \cdot a) \cdot c \quad \text{($\cdot$ is associative)} \\ b = (a \cdot b) \cdot c \quad \text{($\cdot$ is commutative)} \\ b = d \cdot c \quad \text{(hypothesis)} \\ b = c \end{cases}$$