The ring of congruences mod $m$, $\mathbb{Z}_m$. The invertible elements are units if $m$ is prime to $m$.

$$\varphi(m) = \left| \mathbb{Z}_m^\times \right|$$

$$\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$$

$$\varphi(p^a) = p^a - p^{a-1}$$

**THM (Euler)**: $a^{\varphi(m)} \equiv 1 \pmod{m}$ for any $a \in \mathbb{Z}_m^\times$

**Proof**: $A = \{x_1, \ldots, x_{\varphi(m)}\} = \mathbb{Z}_m^\times$ for any $a \in \mathbb{Z}_m^\times$.

$B = \{ax_1, \ldots, ax_{\varphi(m)}\}$

1. Elements $ax_i \not\equiv ax_j \pmod{m}$
2. $a(x_i - x_j) \equiv 0 \pmod{m}$

$\exists b \in \mathbb{Z}_m : ba \equiv 1 \pmod{m} \implies ba(x_i - x_j) \equiv 0 \pmod{m}$

$\iff x_i - x_j \equiv 0 \pmod{m}$

2. $A = B \implies \varphi(m)$

$x_1 \cdot x_2 \cdots x_{\varphi(m)} \equiv a^{\varphi(m)} \equiv 1 \pmod{m}$

Use the fact that $x_i$ are units. "Def. Order of $a$ is smallest $k > 0$ so that $a^k = 1$"
If \( m \) is such that \( a^n = 1 \mod m \) then \( 10 \mid 3112 \mod m \).

**pf:** \( k \leq m \) by def'n of \( k \).
\[
m = k \cdot s + r \quad 1 = a^n = (a^k)^s \cdot a^r = a^r
\]
Since \( 0 \leq r < k \), \( r = 0 \).

For \( \mathbb{Z}_m \), the order of \( a \) is \( \frac{1}{\phi(m)} \).

**Example:** \( m = 125 \), \( \phi(m) = 125 - 25 = 100 \)

So \( 7^{100} \equiv 1 \mod 125 \)

\[
7^{493} = 7^{-7} \quad 7 \cdot 18 \equiv 126 \equiv 1 \mod 125
\]

So \( 7^{493} \equiv (18)^7 \equiv 2 \cdot 3^{14} \)

\( 2^7 = 128 \equiv 3 \mod 125 \) so \( 2^5 \equiv 3 \mod 125 \)

\( 3^{15} = (3^3)^5 = (2 + 25)^5 = 2^5 + (5) 2^4 25 + \ldots \)

\( \equiv 2^5 = 32 \mod 125 \)

---

**FOR APPLICATIONS NEED A MORE GENERAL FORMULA**

**DEF:** A group is a set \( G \) with an operation \( \# \) (usually \( \ast \))

\[
\# : G \times G \to G \quad (a, b) \mapsto a \# b
\]

the product
1. \( a \# (b \# c) = (a \# b) \# c \)

2. \text{unit} \ a \# e = e \# a = a \ \forall a \in G

3. \text{inverse} \ \text{for any} \ a \exists b \in G \ a \# b = b \# a = e.

A subgroup is a set \( H \subseteq G \) such that

(a) \( a, b \in H \implies a \# b \in H \)

(b) \( e \in H \)

(c) \( a \in H \implies a^{-1} \in H \).

\underline{Examples}: \( (\mathbb{Z}_m, \circ) \) is a group

\( (\mathbb{Z}_m, \cdot) \) is \underline{not} a group

For any ring, units form a group.

\( \mathbb{Z} \) \( [\sqrt{3}] \)

\( \mathbb{Z} \ [\sqrt{3}] = \left\{ \pm (2 \pm \sqrt{3})^2 \right\} \)

\underline{THM}: Let \( G \) be any finite group. Then for any subgroup \( H \subseteq G, \)

\( m = \text{size}(H) \mid \text{size}(G) = n \)

\( \text{pf:} \ H = \{ h_1, \ldots, h_m \} \ \text{distinct elements} \).

\( a \in G, \ aH = \{ ah_1, \ldots, ah_m \} \) has \( m \) elements.
\[ a h_i = a h_j \Rightarrow a' a h_i = a' a h_j \Leftrightarrow h_i = h_j \]

2. \[ a H \cap b H = \emptyset \] or the two sets are equal.
\[ x = a h_1 = b h_2 \Rightarrow a = b h_2 h_1^{-1} = bh \]
\[ a H = \{ bh h_1, \ldots, bh h_m \} \]
just a permutation of \( h_1, \ldots, h_m \)

so \( G \) is a union of disjoint sets of size \( m \).
\[ \Rightarrow m = m' s \] i.e. \( m \mid m' \) \[ \exists \]
If \( a \in G, H = \{ a, a^2, \ldots, a^k \} \]
is a subgroup.
\[ a^1 = a^{k-1}, a^2 = a^{k-2}, \ldots \]
\[ a \cdot a = a^k, \quad e = a \]

Then \( k \mid m = |G| \).

As before, if \( a^m = e \), \( k \mid m \)

---

**Lucas-Lehmer Test**

If \( M_l = 2^l - 1 \) is prime, it is called a Mersenne prime

\( l \) must be prime.

\[ M_1 = 2^1 - 1 = 1, \quad M_2 = 2^2 - 1 = 3, \quad M_3 = 2^3 - 1 = 7, \quad M_4 = 15 \]
\[ M_5 = 31, \quad M_6 = 127 \]
Define \( \Delta_1 = 4 \), \( \Delta_{n+1} = \Delta_n^2 - 2 \).

\( \Delta_1 = 4, \Delta_2 = 14, \Delta_3 = 194, \Delta_4 = 37634 \)

\( \Delta_5 = 1416317954 \)

**THM**: \( M_p \) is prime \( \iff \Delta_{p-1} \equiv 0 \, (\text{mod} \, M_p) \)

\( p > 2 \)

\( \Delta_5 \) is huge, but we can simplify:

\[ \Delta_3 \equiv -60 \, (127) \]

\[ \Delta_4 \equiv (-60)^2 - 2 \equiv 42 \, (127) \]

\[ \Delta_5 \equiv (42)^2 - 2 \equiv -16 \, (127) \]

\[ \Delta_6 \equiv (-16)^2 - 2 \equiv 254 \equiv 0 \, (127) \]

so 127 is prime

We will show \( M_3 \mid \Delta_{p-1} \iff M_3 \) is prime

Look at \( R = \mathbb{Z} [\sqrt{3}] \).

Units are \( \pm (2 \pm \sqrt{3})^k \)

\( \alpha = (2 + \sqrt{3}) \quad \beta = (2 - \sqrt{3}) \).

\( \alpha \cdot \beta = 1 \quad \alpha + \beta = 4 = \Delta_1 \)

\( \alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha \beta = \Delta_1^2 - 2 = \Delta_2 \)

\( \alpha^4 + \beta^4 = (\alpha^2 + \beta^2)^2 - 2\alpha^2 \beta^2 = \Delta_2^2 - 2 = \Delta_3 \)
By induction $\alpha^{l-1} + \beta^{l-1} = \delta\ell$

now assume $p | M\ell$ with $1 < p < M\ell$

is a prime. May as well assume $p < \sqrt{M\ell}$

Now look at

$$R = \mathbb{Z}_p [\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}_p\}$$

Say $p | M\ell \mid \alpha_{l-1} = \alpha^2 + \beta^2$.

$$\alpha^2 + \beta^2 \equiv 0 \pmod{p}$$

$$\alpha^2 = -\beta^2 \pmod{p}$$

$$\alpha \cdot \alpha = -\alpha, \beta \equiv -1 \pmod{p}$$

$$\alpha^2 \equiv -1 \pmod{p} \quad (p > 2!)$$

$\alpha \in R^x, \alpha^2 = -1, (\alpha^2) = \alpha^2 = 1$

Order of $\alpha$ is a power of 2. In fact it must be $2^{l-1} = M\ell + 1$.

But $R^x$ has $\leq p^2$ elements $< M\ell$.

Thus such a $p$ cannot exist.