An integral domain is a commutative ring with unit and no zero divisors.

Theorem 19.11: A finite integral domain is a field.

Definition: A ring \( R \) has characteristic \( n > 0 \) if \( nx = 0 \) for all \( x \in R \) and \( n \) is the smallest integer with this property. If there is no such \( n \), we say \( R \) has characteristic 0.

Example: The ring \( \mathbb{Z}/n \mathbb{Z} \) has
characteristic n. If K is a field, its characteristic is either 0 or a prime ≠ p. K stands for Korn.

Thm 20.1 (Little Fermat Theorem)
For any prime p and integer a,
\[ a^p \equiv a \mod p. \]

Proof. Assume \( a \geq 0 \). Proof by induction on a. True for \( a = 0 \). Suppose it is true for some \( n > 0 \). Will show it is true for \( n+1 \):
\[ (n+1)^p = n^p + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} \cdots \binom{p}{p}n + p^p. \]
Note the binomial coeff for $0 < i < \phi$

\[
\binom{\phi}{i} = \frac{\phi!}{i!(\phi-i)!} = \frac{\phi(\phi-1)\cdots(\phi-i+1)}{i!} \text{ something not divisible by } \phi
\]

\[= 0 \mod \phi\]

Hence

\[(n+1)^\phi \equiv n^\phi + 1 \mod \phi\]

\[\equiv n + 1 \mod \phi \text{ by induction}\]

The theorem holds for $n+1$ and hence for all $n \geq 0$.

For $a = -1$

\[(-1)^\phi = (-1)^{\phi-1} = 1 \text{ if } \phi \geq 2\]
\[ a = -n \quad \text{for} \quad n > 1 \]

\[ a^b = (-n)^b = (-1)^b \cdot n^b \]

\[ = (-1)^b \cdot n \quad \text{mod} \quad p \]

\[ = -n = a \quad \text{QED} \]

Application: This leads to a primality test. Suppose \( p \) might be a prime. Calculate \( 2^p \mod p \). If the answer is not 2, then \( p \) is not a prime.
If a prime $p$ does not divide $a$
then $a^{p-1} \equiv 1 \pmod{p}$.

Proof: We know $a^p \equiv a \pmod{p}$

$$a^p - a \equiv 0 \pmod{p}$$

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

In other words, in the ring $\mathbb{Z}/p\mathbb{Z}$,

$$a(a^{p-1} - 1) \equiv 0$$

(a means mod $p$ reduction of $a$)

$\mathbb{Z}/p\mathbb{Z}$ is an integral domain, so

either $a \equiv 0 \pmod{p}$ or $a^{p-1} \equiv 1 \pmod{p}$. We
assumed \( a \neq 0 \) so \( a^{p-1} - 1 \equiv 0 \pmod{p} \) QED.

e.g. \( 250^{691} \equiv 1 \pmod{691} \).

HISTORICAL ASIDE

Fermat was interested in primes of the form \( 2^{2^n} + 1 \).

Exercise: If \( N \) is not a power of 2, then \( 2^N + 1 \) is not a prime.
\[(x^{\text{odd}} + 1) = (x+1)(\text{something})\]
\[(x^5 + 1) = (x+1)(x^4 - x^3 + x^2 - x + 1)\]

\[\begin{array}{cccccc}
\text{n} & 0 & \text{1} & 2 & \text{3} & \text{4} & \text{5} \\
1+2^n & 3 & 5 & 17 & 257 & 65537 & 2^{32} + 1
\end{array}\]

Is \[2^{32} + 1\] a prime? ??

Let \(p\) be a prime that divides
This $\#$. 

\[2^{32} + 1 \equiv 0 \mod p\]

\[2^{32} \equiv -1\]

\[2^{64} = 1\]

\[2^{4k-1} = 1\]

**Conclusion:** $p-1$ is divisible by 64. 

$p = 1 \mod 64$. 

Such primes include
In each case we can calculate

\[ 2^{3^2} \mod p \]

\[ \rightarrow 2^8 \equiv 256 \]

\[ 2^{16} \equiv 154 \mod 641 \]

\[ 2^{32} \equiv 640 = -1 \]

\[ 2^{32} + 1 \text{ is divisible by 641.} \]
If \( p \) is a prime and \( (a, p) = 1 \) then \( a^{p-1} \equiv 1 \pmod{p} \) by \( \gcd \).

Euler's generalization:

If \( (n, a) = 1 \) then
\[
\quad a^{-1} \equiv \frac{1}{a} \pmod{n}
\]
e.g., \( n = 10 \)
\[
\quad 3^4 = 81 \equiv 1 \pmod{10}
\]
7^4 = 2401 \equiv 1 \mod 10
9^2 = 81 \equiv 1 \mod 10
9^4 = 1
14^4 = 1 \mod 10

Def Let \( \phi(n) \) [Euler totient function] be the \# of integers \( k \) with \( 0 < k < n \).
and \( gcd(k, n) = 1 \)

\[
\begin{align*}
\mu(10) &= 4 \\
\mu(4) &= 2 \\
\mu(6) &= 2 \\
\mu(8) &= 4 \\
\mu(12) &= 4
\end{align*}
\]

For a prime \( p \), \( \mu(p) = p - 1 \).
\( \varphi(14) = 6 \) \quad \{1, 3, 5, 9, 11, 13\}

\( \varphi(15) = 8 \) \quad \{1, 2, 4, 7, 8, 11, 13, 14\}

\( \varphi(p^m) = (p-1)p^{m-1} \) \quad p \text{ prime}

\( \varphi(19) = 18 \) \quad \{1, 2, 4, 5, 7, 8\}

Euler's Theorem: If \( \gcd(a, n) = 1 \)

Then \( a^{\varphi(n)} \equiv 1 \pmod{n} \)
Proof. Consider the set
\[ \{ k \mid 0 \leq k < n, \gcd(k, n) = 1 \} \]
It is a group under multiplication and its order is \( \phi(n) \). Hence
\[ k \in \{ k \mid 0 \leq k < n, \gcd(k, n) = 1 \} \]
is a group of invertible elements in \( \mathbb{Z} / n \mathbb{Z} \).
\[ y(p^m) = \frac{p^m}{p^m - 1} \]

\[ \# \text{ in the \# of elements in the set} \]
\[ \left\{ k : 0 < k < p^m, \; \gcd(k, p^m) = 1 \right\} \]
\[ \approx \left\{ k : 0 < k < p^m \right\} \]
\[ \# = (p^m - 1) - (p^m - 1) = p^m - p^{m-1} \]
\( \phi - 1 \) \( \phi_{m-1} = \psi (\phi_m) \)

**Suppose**

\[ n = \phi_1^{m_1} \phi_2^{m_2} \cdots \phi_s^{m_s} \]

where the \( \phi_i \) are distinct primes.

Then

**FUNDAMENTAL THEOREM OF ARITHMETIC**
\[ u(n) = u(\phi_1^{m_1}) u(\phi_2^{m_2}) \]
\[ = (\phi_1^{-1})^{m_1-1} (\phi_2^{-1})^{m_2-1} \]

E.g., \( n = 100 = 2^2 \cdot 5^2 \)
\[ u(100) = u(2^2) u(5^2) \]
\[ = 2 \cdot 20 = 40 \]