$\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ ring.

Thm (Chinese Remainder Theorem).

If $n = m_1 m_2 \cdots m_r$ where $\gcd(m_i, m_j) = 1$ for $i \neq j$.

then $\mathbb{Z}_n = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}$.

(Equivalent version).

Let $m_1, m_2, \cdots, m_r$ be integers which are pairwise coprime. Let $a_1, \cdots, a_r$ be integers s.t. $1 \le a_i < m_i$. Then there exists an integer x s.t.

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

Proof: For $1 \le j \le r$, let $n_j = \prod_{i \neq j} m_i$.

Then $(m_j, n_j) = 1$. and so there exist $s_j, t_j \in \mathbb{Z}$ s.t.

$s_j m_j + t_j n_j = 1$.

Further, $t_j n_j \equiv s_j m_j + t_j n_j = 1 \pmod{m_j}$

Let $x = a_1 t_1 n_1 + a_2 t_2 n_2 + \cdots + a_r t_r n_r$.

Then $x \equiv a_1 t_1 n_1 \pmod{m_1}$

$\equiv a_1 \pmod{m_1}$

$x \equiv a_j t_j n_j \pmod{m_j}$

$\equiv a_j \pmod{m_j}$. $\square$

Eg. ① Let $(m_1, m_2) = (5, 7)$, and $(a_1, a_2) = (2, 3)$ Then

$7 \equiv 2 \pmod 5$

$10 \equiv 3 \pmod 7$

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases} \qquad x = 17.$$

② Let $(m_1, m_2, m_3) = (5, 7, 8)$, and $(a_1, a_2, a_3) = (2, 3, 4)$ Then

$7 \equiv 2 \pmod 5$

$10 \equiv 3 \pmod 7$

$12 \equiv 4 \pmod 8$

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \\ x \equiv 4 \pmod 8 \end{cases} \qquad x = 52$$

Thm (Chinese Remainder Theorem).

If $n = m_1 m_2 \cdots m_r$ where $\gcd(m_i, m_j) = 1$ for $i \neq j$.

then $\mathbb{Z}_n = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}$.

Proof: Define a map

$$\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_r\mathbb{Z}$$

$$a \longmapsto (a + (m_1), \cdots, a + (m_r)).$$

Then φ is a ring homomorphism, with kernel (n).

To complete the proof, we need to prove φ is surjective.

In general, an elt y of $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_r\mathbb{Z}$ is of the form

$(a_1+(m_1),\ a_2+(m_2),\ \cdots,\ a_r+(m_r))$.

Let $I_1=(m_1)=m_1\mathbb{Z}$ and $J=(m_2)\cap(m_3)\cap\cdots\cap(m_r) = (m_2\cdots m_r)$

Then $(m_1, m_2\cdots m_r)=1$. and there exist s,t, s.t. $sm_1+t(m_2\cdots m_r)=1$.

$a_1+b=1$.

Let $x_1=1-a_1=b$ Then $\varphi(x_1)=(x_1+(m_1),\ x_1+(m_2),\ \cdots,\ x_1+(m_r))$

$$= (1-a_1+(m_1),\ b+(m_2),\ \cdots,\ b+(m_r))$$

$$= (1+(m_1),\ (m_2),\ \cdots,\ (m_r))$$

Similarly, there exists x_j s.t. $\varphi(x_j)=((m_1),\cdots,(m_{j-1}),\ 1+(m_j),\ (m_{j+1}),\ \cdots,(m_r))$

Let $z=x_1+x_2+\cdots+x_r$, then

$\varphi(z)=(1+(m_1),\ 1+(m_2),\ \cdots,\ 1+(m_r))$.

Let $x=a_1x_1+a_2x_2+\cdots+a_rx_r$, then

$\varphi(x)=(a_1+(m_1),\ a_2+(m_2),\ \cdots,\ a_r+(m_r))$. So φ is surj. and $\underset{\mathbb{Z}/(n)}{\overset{\|}{\mathbb{Z}/\ker\varphi}} \cong \mathbb{Z}/(m_1)\oplus\cdots\oplus\mathbb{Z}/(m_r)$.

i.e. $\mathbb{Z}_n\cong\mathbb{Z}_{m_1}\oplus\cdots\oplus\mathbb{Z}_{m_r}$. □

<u>Theorem (Chinese Remainder Theorem)</u>

Let R be a ring with identity and $I_1, I_2, \cdots, I_r$ ideals which are pairwise coprime.

Then $R/(I_1\cap\cdots I_r)\cong R/I_1\oplus\cdots\oplus R/I_r$.

Two ideals I,J are <u>coprime</u> if $I+J=R$.

(Consider $(m,n)=1$. $sm+tn=1\Rightarrow(m)+(n)=R$)

<u>Lemma</u> Let I_1, I_2, J be ideals of R. If I_1, I_2 both coprime to J, then I_1I_2 is coprime to J.

<u>Proof</u>: Since $I_1+J=R=I_2+J$, we have $a_1+b_1=1$, $a_2+b_2=1$.

where $a_1\in I_1$, $a_2\in I_2$, $b_1,b_2\in J$.

Then $1=(a_1+b_1)(a_2+b_2)=a_1a_2+(a_1b_2+b_1a_2+b_1b_2)\in I_1I_2+J$.

So $R=I_1I_2+J$. □

R. I,J: ideals of R.

$I+J=\{a+b \mid a\in I,\ b\in J\}$.

$IJ=\{\sum_{\text{finite}} a_ib_j \mid a_i\in I,\ b_j\in J\}$.

If $1\in I$, I ideal. then $r=r\cdot1\in I$, and so $R=I$.

Then, <u>recursively</u>:

Let $I_1, I_2, \cdots, I_t, J$ be ideals of R. If $I_1, I_2, \cdots, I_t$ all coprime to J, then $I_1I_2\cdots I_t$ is coprime to J.

Theorem (Chinese Remainder Theorem)

Let R be a ring with identity and $I_1, I_2, \cdots, I_r$ ideals which are pairwise coprime.

Then $R/(I_1 \cap \cdots I_r) \cong R/I_1 \oplus \cdots \oplus R/I_r$.

Proof: Let φ be a map.

$$\varphi: R \longrightarrow R/I_1 \oplus \cdots \oplus R/I_r$$

$$a \longmapsto (a+I_1, a+I_2, \cdots, a+I_r)$$

Then φ is a ring homo. with $\ker\varphi = I_1 \cap \cdots \cap I_r$. we only need to prove φ is surj.

Let J be an ideal of R, where R is commutative and has identity

① J is a prime ideal if

$J \neq R$, $ab \in J$ then $a \in J$ or $b \in J$.

② J is called maximal ideal if I is an ideal and $I \supsetneq J$, then $I = R$.

Theorem. Let J be an ideal of R. where R is commutative and has identity

(1) J is prime $\Leftrightarrow$ R/J is an integral domain. $R/J = \{\bar{a} \mid a \in R\}$.

(2) J is maximal $\Leftrightarrow$ R/J is a field.

In particular, for commutative ring with identity, a maximal ideal is a prime ideal.

(Since a field is an integral domain).

Proof: (1) J is prime

$\Leftrightarrow$ $ab \in J$ implies $a \in J$ or $b \in J$

$\Leftrightarrow$ $\bar{a}\bar{b} = \bar{0}$ implies $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$

$\Leftrightarrow$ R/J is an integral domain.

Recall: If R is commutative with identity and has no zero factor, then R is an integral domain 整环.

(R should also have at least 2 elts and identity for multiplication). $0 \neq 1$

(2) J is maximal

$\Leftrightarrow$ $(a) + J = (1)$ $\forall a \in R \setminus J$.

$\Leftrightarrow$ $(\bar{a}) = (\bar{1})$ $\forall a \in R \setminus J$.

$\Leftrightarrow$ $\bar{a} \cdot \bar{b} = \bar{1}$ for some $\bar{b} \in R/J$.

$\Leftrightarrow$ $\bar{b} = \bar{a}^{-1}$

$\Leftrightarrow$ R/J is a field. $\square$.

$\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$.

$\downarrow$

$\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z},\ n \neq 0\}$.

with $\frac{m_1}{n_1} \cdot \frac{m_2}{n_2} = \frac{m_1 m_2}{n_1 n_2}$.

$\frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1 n_2 + n_1 m_2}{n_1 n_2}$.

Let R be an integral domain.

Define: $S = \{(a,b) \mid a, b \in R,\ b \neq 0\}$. and $(a_1, b_1) \cdot (a_2, b_2) = (a_1 b_1, a_2 b_2)$.

$(a_1, b_1) + (a_2, b_2) = (a_1 b_2 + b_1 a_2,\ b_1 b_2)$. | $\frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1 n_2 + n_1 m_2}{n_1 n_2}$.

If $(a_1, b_1) = (a_2 r, b_2 r)$, then identify (a_1, b_1) and (a_2, b_2). | $\frac{2}{4} = \frac{1 \times 2}{2 \times 2} = \frac{1}{2}$

$(2, 4) = (1, 2)$

Then, $(S, +, \times)$ is a ring. a comm. ring. a comm. integral domain.

a field. called the <u>fractional field</u> of R.

Let R be a commutative ring with identity.

Let $T \subset R$ s.t. none of the elts. of T is a zero divisor of R. (also require T to be closed under multiplication.

Let $S = \{(a,b) \mid a \in R, b \in T\}$. Then S is a ring and $R \leq S$. denoted by $T^{-1}R$.