中国剰余定理 (chinese remainder theorem)

目次

<u>定義 **1 :** イデアル **(ideal)**</u> R を可換環とする。以下を見たす R の部分集合 I を R 上のイデアルという。

(I1) $\forall x, y \in I, x + y \in I$

(I2) $\forall x \in I, a \in R, ax \in I$

<u>系 **1 :** 単項イデアル **(principal ideal)**</u> 可換環 R のある元 $m \in R$ によって書かれる集合 I

$$I = \{am \mid a \in R\}$$

はイデアルとなる。この I を m を生成元とする単項イデアルという。また、m を生成元とする単項イデアルを mR と書くこともある。

<u>定義 **2 :** 剰余類 **(residue class)**</u> 可換環 R 上のイデアル I と任意の $x \in R$ に対して

$$x + I = \{x + a \mid a \in I\}$$

を x を代表元とする剰余類という。

<u>定理 **1 :**</u> ある $x, y \in R$ が $x - y \in I$ であるとき、$x + I = y + I$ である。

Proof. I の生成元が m であるとする。まず定義より $x + I$ の任意の元 a はある $q \in R$ によって

$$a = x + mq$$

と書くことができる。ここで仮定より、ある p によって $x - y = mp \Leftrightarrow x = y + mp$ となる。この x を代入すると

$$\begin{aligned} a &= y + mp + mq \\ &= y + m(p + q) \end{aligned}$$

となり、$a \in y+I$ が得られた。ここで a は任意の $x+I$ の元であるため $a \in x+I \Rightarrow a \in y+I$ が示された。同様にして $a \in y+I \Rightarrow a \in x+I$ が示される。以上より示された。 □

<u>定義 **3 :** 剰余環 **(quotient ring)**</u> 可換環 R 上のイデアル I に対して

$$R/I = \{x+I \mid x \in R\}$$

として書かれる集合 R/I を R 上の剰余環という。

<u>定理 **2 :**</u> 可換環 R 上の剰余環 R/I は可換環となる。

Proof. □

<u>定理 **3 :**</u> hoge

<u>定理 **4 :** 中国剰余定理 **(Chinese Remainder Theorem)**</u> ある剰余環 Z/mZ に