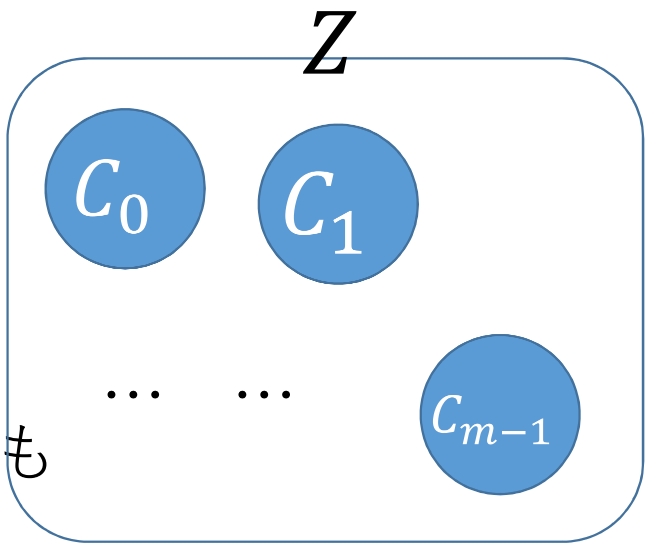
剰余類

多くの暗号システムは、法演算を用いて構成されると述べたが、
より厳密には、剰余類環や剰余類体の上で定義される。

剰余類とは

- 自然数mを一つ定め、このmを法とする合同演算によって、整数Zを等しいもの同士に分類することを考える。
  明らかに、整数Zはm個の集合$\{C_0, C_1, \ldots, C_{m-1}\}$に分類され、どの集合にも含まれない整数や、複数の集合に含まれる整数は存在しないことがわかる。
- 集合$C_i (i = 0,1, \ldots, m-1)$を剰余類、また
- 剰余類の集合$\{C_0, C_1, \ldots, C_{m-1}\}$を$Z_m$と表す
- （例）$m = 2$とすれば、剰余類C_0は偶数を、
  C_1は奇数を表すことになる。また、
  $Z_2 = \{C_0, C_1\}$である。
- 「余り」が定義できれば、整数の演算以外でも剰余類が定義できる（例、多項式の剰余類）



剰余類の計算

- 剰余類同士の計算（例えば加算）$C_i + C_j$を以下のように定義する。
- 任意の$x \in C_i$、および任意の$y \in C_j$を選び、$z = x + y$を求める。このとき、$z \in C_k$であるなら、$C_i + C_j = C_k$と定義する。
- この定義で、xとyをどのように選んでも結果は同じになる（なぜか。合同式の性質を使って各自考えてみよ）
- 乗算（$C_i \times C_j$）についても同様に定義できる。
- （例）$m = 5$とする。$C_1 + C_3$を求める。$x = 21 \in C_1$、$y = -2 \in C_3$と選ぶ。$z = x + y = 19 \in C_4$なので、$C_1 + C_3 = C_4$である。他の、x, yについても同じ結果になることを確認しよう。

剰余類の表現

- 剰余類$\{C_o, C_1, \dots, C_{m-1}\}$は、簡単のため、単に、$Z_m = \{0,1,\dots,m-1\}$と書くことが多い。
- 剰余類C_iの添え字iは、C_iに含まれる整数であれば何でもよい。
（例）$m = 5$のとき、$z_5 = \{10, 1, -3, 48, -1\}$
- $Z_m = \{a_0, a_1, \dots, a_{m-1}\}$と表されるとき、$\{a_0, a_1, \dots, a_{m-1}\}$を完全代表系と呼ぶ。各$a_i$は代表元と呼ばれる。
- よく使われる完全代表系（応用によって便利なものを使う）
  - $Z_m = \{0,1,2,\dots,m-1\}$
  - $Z_m = \{1,2,3,\dots,m\}$
  - $Z_m = \{-\left\lfloor\frac{m-1}{2}\right\rfloor, -\left\lfloor\frac{m-1}{2}\right\rfloor + 1, \dots, -1,0,1,\dots,\left\lfloor\frac{m}{2}\right\rfloor - 1, \left\lfloor\frac{m}{2}\right\rfloor\}$
- 以降の説明では複数の完全代表系を混ぜて使うこともある。
（例）$x^2 = 1(mod\ 5)$の解は、$x = \pm1(mod\ 5)$である（$x = 1,4(mod\ 5)$である）

完全代表系の性質

- ［定理３］ $\{a_0, a_1, \ldots, a_{m-1}\}$を$m$を法とする完全代表系とする。このとき、$(a, m) = 1$ならば、$\{a \cdot a_0, a \cdot a_1, \ldots, a \cdot a_{m-1}\}$も完全代表系である。
- （証明）$a \cdot a_i (i = 0,1, \ldots, m-1)$が$m$を法として相異なることを言えばよい。背理法による。ある$i \neq j$について、

$$a \cdot a_i = a \cdot a_j \pmod m$$

であったとする。$(a, m) = 1$であるので、定理２により両辺をaで割って、$a_i = a_j \pmod m$を得る。これは、$\{a_0, a_1, \ldots, a_{m-1}\}$が完全代表系であることに矛盾する。よって証明できた。

定理３の例

- 法$m = 10$とする。完全代表系（の一つ）は$\{0,1,2,3,4,5,6,7,8,9\}$である。
- mと互いに素な数$a = 3$とし、各代表元に乗ずると、$\{0,3,6,9,12,15,18,21,24,27\}$となり、これはまた完全代表系になっていることがわかる。実際、これらの数のmによる剰余を求めると、$\{0,3,6,9,2,5,8,1,4,7\}$であり、全て異なることがわかる。
- 定理を満たさない例として、mと互いに素でない数$a' = 2$とし、これを各代表元に乗ずると、$\{0,2,4,6,8,10,12,14,16,18\}$となり、これは完全代表系ではない。実際、これらの数のmによる剰余を求めると、$\{0,2,4,6,8,0,2,4,6,8\}$であり、同じ剰余を持つものが複数あることがわかる。

既約剰余類とは

- 剰余類$Z_m = \{0,1,\dots,m-1\}$について、
$$\tilde{Z}_m = \{i \mid (i,m) = 1, i \in Z_m\}$$
を既約剰余類と呼ぶ。つまり、剰余類Z_mの元のなかで、mと互いに素な剰余類のことである。
- （例１）$m = 15$のとき、既約剰余類$\tilde{Z}_{15} = \{1,2,4,7,8,11,13,14\}$
$\widetilde{Z_{15}}$の要素の数は8個だが、一般に$\tilde{Z}_m$の要素の個数はどうか？
- （例２）$m = 11$のとき、$\tilde{Z}_{11} = \{1,2,3,4,5,6,7,8,9,10\}$
一般に、$m = p$（素数）のとき、$\tilde{Z}_p = \{1,2,\dots,p-1\}$となる。
（なぜか、考えてみよう）

既約剰余類の性質

- 既約剰余類についても定理３が成り立つ
- [定理３']　既約剰余類$\tilde{Z}_m$の代表系を$\{a_1, a_2, \dots, a_n\}$とする。ただし、$n = |\tilde{Z}_m|$（$\tilde{Z}_m$の要素の数）である。このとき、$(a, m) = 1$ならば、$\{a \cdot a_1, a \cdot a_2, \dots, a \cdot a_n\}$も既約剰余類$\tilde{Z}_m$の代表系である。
- （証明）$(a, m) = 1$かつ$(a_i, m) = 1$であるから、$(a \cdot a_i, m) = 1$であり、$a \cdot a_i$は既約剰余類$\tilde{Z}_m$の代表元の一つである。また、任意の$i \neq j$について $a \cdot a_i \neq a \cdot a_j (mod\, m)$であることは定理3と同様に示せる。
- （例）$\tilde{Z}_{15} = \{1,2,4,7,8,11,13,14\}$に対して、$a = 2$とすると、$\{2,4,8,14,16,22,26,28\}$は、$\tilde{Z}_{15}$の代表系になっている。
  実際、これらの要素について15の剰余を求めると
  $\{2,4,8,14,1,7,11,13\}$となり全て異なっている。