1　合同式 (congruence) と基本定理

$$a \equiv b \pmod{m} \tag{1}$$

a を m で割った余りと b を m で割った余りが等しいことを、法 m について合同であるという。

加算と積に関しては、通常の整数に対する規則が成立する。a を m で割った商を q_a 余りを r_a とすると、

$$a = q_a m + r_a \tag{2}$$

同様に、

$$b = q_b m + r_b \tag{3}$$

と一意的に記述できる。よって、

$$a \pm b = (q_a \pm q_b)m + (r_a \pm r_b) \tag{4}$$

また、

$$\begin{aligned} ab &= (q_a m + r_a)(q_b m + r_b) \\ &= (q_a q_b m + q_a r_b + q_b r_a)m + r_a r_b \end{aligned} \tag{5}$$

であるから、合同式を使って、

$$a \equiv r_a \pmod{m} \tag{6}$$
$$b \equiv r_b \pmod{m} \tag{7}$$
$$ab \equiv r_a r_b \pmod{m} \tag{8}$$

と記述できる。$b \equiv c$ の場合、

$$a \pm b \equiv a \pm c \pmod{m} \tag{9}$$
$$ab \equiv ac \pmod{m} \tag{10}$$

と整数で成立する一般的な加減算と積の規則が成立することは、容易に証明できる。しかし、割り算に関しては注意を要する。

$$c = q_c m + r_c$$

としよう。そうすると、

$$ac = (q_a q_c m + q_a r_c + q_c r_a)m + r_a r_c$$

と記述できる。ここで、$ab \equiv ac \pmod{m}$ であった場合、

$$r_a r_b \equiv r_a r_c \pmod{m}$$

であることは明らかであるが、一般的には、

$$r_b \neq r_c$$

である。よって、共通項での割り算は一般的にはできない。具体的には、$m = 6, r_a = 3, r_b = 1, r_c = 3$ の場合、

$$\begin{aligned} r_a r_b &= 3 \\ r_a r_c &= 9 \equiv 3 \pmod 6 \end{aligned}$$

であるから、

$$r_a r_b \equiv r_a r_c \equiv 3 \pmod 6$$

が成立する。しかし、$r_b \neq r_c$ つまり、$b \not\equiv c \pmod 6$ である。

1.1 基本定理２

a と b の最大公約数 (greatest common divisor) を $\gcd(a,b)$ もしくは単に (a,b) で表す。

さてここで、a と m の最大公約数 $(a,m) = g$ とし、$ab \equiv ac \pmod m$ が成立するとしよう。

$$ab - ac \equiv 0 \pmod m$$

が成立するので、m で割り切れる数であり、

$$ab - ac = mq$$

と書ける。ここで q はある整数である。$a = a'g, m = m'g$ と書けるので、

$$ab - ac = a'g(b-c) = m'gq$$

よって、

$$a'(b-c) = m'q$$

が成立する。定義により、a' と m' は互いに素の関係 ($(a', m') = 1$) であるから、

$$b - c = m'(q/a') = m'q'$$

となる q' が存在する。よって、

$$\begin{aligned} b - c &\equiv 0 \pmod{m'} \\ b &\equiv c \pmod{\frac{m}{g}} \end{aligned} \tag{11}$$

が成立する。

1.2 基本定理３

$(m,n) = 1, a \equiv b \pmod m, a \equiv b \pmod n$ ならば、$a \equiv b \pmod{mn}$ である。

$$a - b = mq = nq'$$

と記述できる。m, n は互いに素であるから、$q = ns$ と記述できるある整数 s が存在する。よって、

$$a - b = mns$$

と書ける。つまり、$a-b$ は mn の整数倍であるから、

$$a-b \equiv 0 \pmod{mn}$$

よって、

$$a \equiv b \pmod{mn} \tag{12}$$

それでは、$(m,n)=1, a \equiv b \pmod{mn}$ ならば、$a \equiv b \pmod{m}, a \equiv b \pmod{n}$ が成立するかどうか検証してみよう。

$$a-b \equiv 0 \pmod{mn}$$

よって、

$$\begin{aligned} a-b &= mns \\ &= ms' \\ &= ns'' \end{aligned}$$

と記述できるある整数 s, s', s'' が存在する。よって、

$$\begin{aligned} a &\equiv b \pmod{m} \\ a &\equiv b \pmod{n} \end{aligned}$$

が成立する。

1.3 Euclid の互除法

整数 a と b の最大公約数 d を求めることを考える。ここで、$a > b$ とすると、

$$a = a'd, \quad b = b'd$$

と書ける。また、a を b で割った商を q、余りを r とすると、

$$a = bq + r$$

よって、

$$r = a - bq = a'd - b'dq = d(a' - b'q)$$

ここで、$r = 0$ の場合、最大公約数 $d = b$ であることが確定する。$r > 0$ の場合、

$$a' - b'q \equiv r' > 0$$

であるから、

$$r = r'd$$

と書け、b と r の公約数が d であることがわかる。

さて、b と r の最大公約数を d' とすると、

$$b = b''d', \quad r = r''d'$$

よって、

$$\begin{aligned} a &= bq + r \\ &= b''d' + r''d' \\ &= d'(b'' + r'') \end{aligned}$$

であるから、d' は a と b の公約数でもあることがわかる。よって、

$$d \geqq d'$$

また、b と r の公約数が d であることから、

$$d' \geqq d$$

よって、

$$d = d'$$

となり、

$$(a, b) = (b, r)$$

が成立する。つまり、ユークリッドの互除法によって最後まで余りに最大公約数が約数として残るので、最後に残った余りが最大公約数となる。

ユークリッドの互除法は超高速に最大公約数を求めることができることで知られている。($O(\log n)$)

ところで、最大公約数は、素因数分解によっても求めることができるので、素因数分解で求めてもよいと思っている人が多い。しかし、取り扱う数 n が非常に大きな数の場合、この素因数分解法は非常に時間が掛かる超難題として知られている。そのため、大きな数の最大公約数を求める場合、ユークリッドの互除法以外の選択肢は無くなる。