高校数学の復習 12　合同式

整数問題を解くときに威力を発揮するのが合同式になります。こちらは、高校の課程によっては習っていない方もいるかもしれません。私も皆様とは、年代はだいぶ違いますが、高校時代に履修してきませんでした。しかし、大学で数学を、特に情報系の数学を学ぶ上で大変活躍する知識になりました。けっして難しくはありませんので、この際しっかりとマスターしてみましょう。

整数 a と b があって、整数 c で割り算をしたときの剰余(余り)が等しいときに、

$a \equiv b \pmod{c}$　**a と b は c を法として合同**といいます。

合同の例

$8 \equiv 1 \pmod{7}$

$14 \equiv 1 \pmod{13}$

$-1 \equiv 2 \pmod{3}$

ちょっとわかりにくいですが、−1 は３で割って２余りということになります。

$-1 = 3 \times (-1) + 2$

合同式の基本的な性質を示します。

$a \equiv b$ で $c \equiv d$ ならば

$a+c \equiv b+d$　合同どうし足しても等号がなりたつ。

$a-c \equiv b-d$　合同どうし引いても等号がなりたつ。

$ac \equiv bd$　合同どうし定数を掛けても等号がなりたつ。

$a^n \equiv b^n$ なら $a \equiv b$ が成り立つし、逆も成り立つ。

さらに、

$ka \equiv kb \pmod{c}$ のときに、**k と c が互いに素であれば除法が成り立つ。**

⇒ $a \equiv b$

例題 1　合同式の性質を使って次の式を解いてみましょう。

$29a \equiv 13 \pmod{7}$

まず左辺の 13 は mod7 で考えると、6

$29a \equiv 6$　(1)

一方 28 a は 7 の倍数なので

$28a \equiv 0$　　(2)

(1)-(2)を計算すると、

$a \equiv 6$

つまり、a は 7 で割って、6 余る数である。

検算してみよう。 $a=7k+6$　(k は整数)として与式に代入する。

$29(7k+6)=29 \cdot 7k+174 = 7 \cdot (29k+23) + 13$

となり、7 の倍数として 13 余ることがわかる。

例題 2　合同式の性質を使って次の式を解いてみましょう。

$17x \equiv 27 \mod 14$

まず、

$14x \equiv 0 \mod 14$

を考えて、与式から引き算をします。

$3x \equiv 27 \mod 14$

ここで 14 と 3 は互いに素ですから、

$x \equiv 9 \mod 14$

となります。

検算してみましょう。 $x=14k+9$　k は整数とします。

与式に代入すると、

$17(14k+9) = 17 \cdot 14k + 153 = 17 \cdot 14k + 14 \times 9 + 27 = 14(17k+9)+27$

で余りが 27 になることが分かります。

練習問題 1　次の合同式を解きなさい。変数はすべて整数とします。

(1) $19a \equiv 39 \pmod{14}$　(2) $35b \equiv 128 \pmod{27}$　(3) $17c \equiv -25 \pmod{7}$

解答

(1) $19a \equiv 39 \pmod{14}$

これも左辺の 39 ですが、14 で割って 11 余りますので、小さな数字にしていきましょう。

$19a \equiv 11$　①

また整数 $14a$ は 14 の倍数ですから、mod14 でゼロ。

$14a \equiv 0$　②

①－②より、

$5a \equiv 11$

ここで、左辺に 14 の整数倍を足すか引くかして、5 で割り切れないかを考えます。

$5a \equiv 11 + 14 = 25$

ここで、両辺を 5 で割りたいのですが、割る数と法の 14 が互いに素なので、わることができます。

$a \equiv 5 \pmod{14}$

つまり, a は 14 で割ったら 5 余る数になります。

検算ですが、$a=14m+5$ （m は整数）として与式に代入します。

$19(14m+5)=19 \cdot 14m+95=19 \cdot 14m+56+39=14(19m+4)+39$

たしかに、39 余ることが分かりましたね。

(2) $35b \equiv 128 \pmod{27}$

まず、右辺の 128 は 27 で割ると、20 余ります。したがって、

$35b \equiv 20$

5 で両辺を割りたいですが、法の 27 とは互いに素ですので割ることができます。

$7b \equiv 4$

ここで、27 の整数倍を足すなり引くなりして、7 で割れないかを検討します。

ここは 27 の 4 の倍数 108 をたすと、右辺が 112 になり、7 で割り切れます。

$7b \equiv 4 + 108$（7 の倍数）$\equiv 112$

法の 27 と 7 は互いに素なので、

$b \equiv 16$

と求まります。

検算も自分でやってみましょう。$b=27m+16$ と置いて計算すると、

$35b=35(27m+16)=35 \cdot 27m+560=35 \cdot 27m+432+128=35(27m+16)+128$

と、確かに 128 余ります。

(3) $17c \equiv -25 \pmod{7}$

右辺がーになっていても、余りは定義できます。こちらも右辺に 7 の倍数を足してわかりやすい数字にしましょう。ここは 7 の倍数である 28 を足します。

$17c \equiv -25+28 \equiv 3$ ①

さて、左辺を整理します。左辺の 17 を減らすことを考えます。ここで、$14c$ は 7 の倍数になりますので、 ②

$14c \equiv 0$

①－②より、

$3c \equiv 3$

となります。ここで法の 7 と 3 は互いに素ですから、両辺 3 で割り切れます。

$c \equiv 1$

ここでも練習ですから検算します。$c=7m+1$ と置いて、与式の左辺を計算します。

$17(7m+1)=17\cdot 7m+17=17\cdot 7m+17+25-25=17(7m+6)-25$

確かに正しいことがわかりました。

合同式を使うとこんな問題も解くことができます。

例題 3　累乗の余りの計算

次の数を 13 で割った余りを計算しなさい。

20^{111}

解答

この問題を解くのに、二項定理を使うか、合同式をつかうのですが、こう考えましょう。

試しに 20 の mod13 を計算すると、20 を 13 で割れば 7 になりますね。

$20^{111} \equiv 7^{111}$

ここで、試しに小さい数で 7 の累乗を計算してみます。そして、mod13 で 1 が出てくるまで繰り替えします。

$7^1 \equiv 7 \pmod{13}$

$7^2 \equiv 49 \equiv 10 \pmod{13}$

$7^3 \equiv 343 \equiv 5 \pmod{13}$

$7^4 \equiv 10^2 \equiv 9 \pmod{13}$　　ここは、7^4 を直接計算するより、二行前の式の結果使って簡単にする。

$7^5 \equiv 10\times 5 \equiv 50 \equiv 11 \pmod{13}$　　これも 7^2 と 7^3 の式を使う

$7^6 \equiv 5\times 5 \equiv 25 \equiv 12 \equiv -1 \pmod{13}$

さあここで、－1 がでてきましたが、これは $7^{12} \equiv 7^6 \cdot 7^6 \equiv 1$

なることが分かりました。つまり 7^{12} は 13 で割って 1 余りますので、

$7^{111} \equiv 7^{108}\cdot 7^3 \equiv (7^{12})^9 \cdot 7^3 \equiv 1^9 \cdot 7^3 \equiv 5$

つまり、5 余ります。（答え）

練習問題 2　次の数を 10 で割った余りを計算しましょう。

13^{21}

答え　3 になります。

これも先ほどの例の通り小さい数で累乗を計算してきましょう。

$13^1 \equiv 3 \pmod{10}$

$13^2 \equiv 139 \equiv 9 \pmod{10}$

$13^3 \equiv 13^1 \cdot 13^2 \equiv 3 \cdot 9 \equiv 7 \pmod{10}$

$13^4 \equiv 9 \cdot 9 \equiv 1 \pmod{10}$

ここで、13^4 を一かたまりでみれば、余り 1 になります。

$13^{21} \equiv (13^4)^5 \cdot 13 \equiv 13 \equiv 3$

したがって、3 余ることが示されました。

さあいかがでしたか。

合同式は工学の分野で素数を用いた暗号生成と解読などに使われています。

次回も合同式を用いた応用問題に取り組んでまいりましょう。